Dell Networking W-Series Instant 6.4.0.2-4.1

User Guide

Copyright

© 2014 Aruba Networks, Inc. Aruba Networks trademarks include , Aruba Networks®, Aruba Wireless Networks®, the registered Aruba the Mobile Edge Company logo, and Aruba Mobility Management System®. Dell™, the DELL™ logo, and PowerConnect™ are trademarks of Dell Inc.

All rights reserved. Specifications in this manual are subject to change without notice.

Originated in the USA. All other trademarks are the property of their respective owners.

Open Source Code

Certain Aruba products include Open Source software code developed by third parties, including software code subject to the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), or other Open Source Licenses. Includes software from Litech Systems Design. The IF-MAP client library copyright 2011 Infoblox, Inc. All rights reserved. This product includes software developed by Lars Fenneberg, et al. The Open Source code used can be found at this site:

http://www.arubanetworks.com/open_source

Legal Notice

The use of Aruba Networks, Inc. switching platforms and software, by all individuals or corporations, to terminate other vendors' VPN client devices constitutes complete acceptance of liability by that individual or corporation for this action and indemnifies, in full, Aruba Networks, Inc. from any and all legal actions that might be taken against it with respect to infringement of copyright on behalf of those vendors.

Contents 3
About this Guide 28
Intended Audience 28
Related Documents 28
Conventions 28
Contacting Dell 29
About Instant 30
Instant Overview 30
Supported Devices 30
Instant UI 31
Instant CLI 31
What is New in Instant 6.4.0.2-4.1 33
Setting up a W-IAP 35
Setting up Instant Network 35
Connecting a W-IAP 35
Assigning an IP address to the W-IAP 35
Assigning a Static IP 36
Connecting to a Provisioning Wi-Fi Network 36
W-IAP Cluster 36
Disabling the Provisioning Wi-Fi Network 37
Logging in to the Instant UI 37
Regulatory Domains 38
Country Code 38
Specifying Country Code 41
Accessing the Instant CLI 41
Connecting to a CLI Session 42
Applying Configuration Changes 42
Using Sequence Sensitive Commands 43

Instant User Interface 44
Login Screen 44
Logging into the Instant UI 44
Viewing Connectivity Summary 44
Language 44
Main Window 45
Banner 45
Search 45
Tabs 45
Networks Tab 46
Access Points Tab 46
Clients Tab 47
Links 47
New Version Available 47
System 48
RF 49
Security 50
Maintenance 51
More 52
VPN 52
IDS 53
Wired 54
Services 54
DHCP Server 55
Support 56
Help 57
Logout 57
Monitoring 57
Info 57
RF Dashboard 59
RF Trends 60
Usage Trends 61
Mobility Trail 66

Client Match 66
AppRF 67
Spectrum 67
Alerts 67
IDS 71
AirGroup 72
Configuration 72
W-AirWave Setup 73
Pause/Resume 73
Views 73
Initial Configuration Tasks 74
Basic Configuration Tasks 74
Modifying the W-IAP Name 74
In the Instant UI 75
In the CLI 75
Updating Location Details of a W-IAP 75
In the Instant UI 75
In the CLI 75
Configuring a Preferred Band 75
In the Instant UI 75
In the CLI 75
Configuring Virtual Controller IP Address 76
In the Instant UI 76
In the CLI 76
Configuring Timezone 76
In the Instant UI 76
In the CLI 76
Configuring an NTP Server 76
In the Instant UI 77
In the CLI 77
Enabling AppRF Visibility 77
Changing Password 77

In the Instant UI 77
In the CLI 77
Additional Configuration Tasks 78
Configuring Virtual Controller VLAN 78
In the Instant UI 79
In the CLI 79
Configuring Auto Join Mode 79
Enabling or Disabling Auto Join Mode 79
In the Instant UI 79
In the CLI 79
Configuring Terminal Access 80
In the Instant UI 80
In the CLI 80
Configuring Console Access 80
In the Instant UI 80
In the CLI 80
Configuring LED Display 81
In the Instant UI 81
In the CLI 81
Configuring Additional WLAN SSIDs 81
Enabling the Extended SSID 81
In the Instant UI 81
In the CLI 82
Preventing Inter-user Bridging 82
In the Instant UI 82
In the CLI 82
Preventing Local Routing between Clients 82
In the Instant UI 82
In the CLI 83
Enabling Dynamic CPU Management 83
In the Instant UI 83
In the CLI 83

Customizing W-IAP Settings 84
Modifying the W-IAP Hostname 84
In the Instant UI 84
In the CLI 84
Configuring Zone Settings on a W-IAP 84
In the Instant UI 85
In the CLI 85
Specifying a Method for Obtaining IP Address 85
In the Instant UI 85
In the CLI 86
Configuring External Antenna 86
EIRP and Antenna Gain 86
Example 86
Configuring Antenna Gain 86
In the Instant UI 86
In the CLI 87
Configuring Radio Profiles for a W-IAP 87
Configuring ARM Assigned Radio Profiles for a W-IAP 87
Configuring Radio Profiles Manually for W-IAP 87
In the CLI 88
Configuring Uplink VLAN for a W-IAP 88
In the Instant UI 88
In the CLI 89
Master Election and Virtual Controller 89
Master Election Protocol 89
Preference to a W-IAP with 3G/4G Card 89
Preference to a W-IAP with Non-Default IP 90
Viewing Master Election Details 90
Manual Provisioning of Master W-IAP 90
Provisioning a W-IAP as a Master W-IAP 90
In the Instant UI 90
In the CLI 90

Adding a W-IAP to the Network 91
Removing a W-IAP from the Network 91
VLAN Configuration 92
VLAN Pooling 92
Uplink VLAN Monitoring and Detection on Upstream Devices 92
Wireless Network Profiles 93
Configuring Wireless Network Profiles 93
Network Types 93
Configuring WLAN Settings for an SSID Profile 93
In the Instant UI 94
In the CLI 96
Configuring VLAN Settings for a WLAN SSID Profile 97
In the Instant UI 97
In the CLI 98
Configuring Security Settings for a WLAN SSID Profile 99
Configuring Security Settings for an Employee or Voice Network 99
In the Instant UI 99
In the CLI 103
Configuring Access Rules for a WLAN SSID Profile 104
In the Instant UI 105
In the CLI 105
Example 106
Configuring Fast Roaming for Wireless Clients 106
Opportunistic Key Caching 106
Configuring a W-IAP for OKC Roaming 107
In the Instant UI 107
In the CLI 107
Fast BSS Transition (802.11r Roaming) 107
Configuring a W-IAP for 802.11r support 108
In the Instant UI 108
In the CLI 108
Example 108
Radio Resource Management (802.11k) 108

Beacon Report Requests and Probe Responses 109
Configuring a WLAN SSID for 802.11k Support 109
In the Instant UI 109
In the CLI 109
Example 109
BSS Transition Management (802.11v) 109
Configuring a WLAN SSID for 802.11v Support 110
In the Instant UI 110
In the CLI 110
Example 110
Editing Status of a WLAN SSID Profile 110
In the Instant UI 110
In the CLI 110
Editing a WLAN SSID Profile 110
Deleting a WLAN SSID Profile 111
Wired Profiles 112
Configuring a Wired Profile 112
Configuring Wired Settings 112
In the Instant UI 112
In the CLI 113
Configuring VLAN for a Wired Profile 114
In the Instant UI 114
In the CLI 114
Configuring Security Settings for a Wired Profile 115
Configuring Security Settings for a Wired Employee Network 115
In the Instant UI 115
In the CLI 115
Configuring Access Rules for a Wired Profile 116
In the Instant UI 116
In the CLI 116
Assigning a Profile to Ethernet Ports 117
In the Instant UI 117
In the CLI 117

Editing a Wired Profile 117
Deleting a Wired Profile 118
Link Aggregation Control Protocol for W-IAP220 Series 118
Understanding Hierarchical Deployment 119
Captive Portal for Guest Access 120
Understanding Captive Portal 120
Types of Captive Portal 120
Walled Garden 121
Configuring a WLAN SSID for Guest Access 121
In the Instant UI 121
In the CLI 124
Configuring Wired Profile for Guest Access 125
In the Instant UI 125
In the CLI 126
Configuring Internal Captive Portal for Guest Network 126
In the Instant UI 127
In the CLI 128
Configuring External Captive Portal for a Guest Network 129
External Captive Portal Profiles 129
Creating a Captive Portal Profile 129
In the Instant UI 129
In the CLI 130
Configuring an SSID or Wired Profile to Use External Captive Portal Authentication 131
In the Instant UI 131
In the CLI 132
Configuring External Captive Portal Authentication Using ClearPass Guest 132
Creating a Web Login page in ClearPass Guest 133
Configuring RADIUS Server in Instant UI 133
Configuring Guest Logon Role and Access Rules for Guest Users 133
In the Instant UI 133
In the CLI 134
Example 135

Configuring Captive Portal Roles for an SSID 135
In the Instant UI 135
In the CLI 137
Configuring Walled Garden Access 138
In the Instant UI 138
In the CLI 138
Disabling Captive Portal Authentication 138
Authentication and User Management 140
Managing W-IAP Users 140
Configuring Authentication Parameters for Management Users 141
Configuring a TACACS+ Server Profile for Management User Authentication 141
In the Instant UI 141
In the CLI 142
Configuring Administrator Credentials for the Virtual Controller Interface 142
In the Instant UI 142
In the CLI 143
Configuring Guest Management Interface Administrator Credentials 144
In the Instant UI 144
In the CLI 144
Configuring Users for Internal Database of a W-IAP 144
In the Instant UI 144
In the CLI 145
Configuring the Read-Only Administrator Credentials 146
In the Instant UI 146
In the CLI 146
Adding Guest Users through the Guest Management Interface 146
Understanding Authentication Methods 147
802.1X authentication 147
MAC authentication 147
MAC authentication with 802.1X authentication 147
Captive Portal Authentication 148
MAC authentication with Captive Portal authentication 148

802.1X authentication with Captive Portal Role 148
WISPr authentication 148
Supported EAP Authentication Frameworks 148
Authentication Termination on W-IAP 149
Supported Authentication Servers 149
Internal RADIUS Server 150
External RADIUS Server 150
RADIUS Server Authentication with VSA 150
Dynamic Load Balancing between Two Authentication Servers 154
Understanding Encryption Types 154
WPA and WPA2 154
Recommended Authentication and Encryption Combinations 155
Support for Authentication Survivability 155
Configuring Authentication Survivability 156
In the Instant UI 156
Important Points to Remember 156
In the CLI 156
Configuring Authentication Servers 157
Configuring an External Server for Authentication 157
In the Instant UI 157
In the CLI 160
Configuring Dynamic RADIUS Proxy Parameters 161
Enabling Dynamic RADIUS Proxy 161
In the Instant UI 161
In the CLI 162
Configuring Dynamic RADIUS Proxy Parameters for Authentication Servers 162
In the Instant UI 162
In the CLI 162
Associate the Authentication Servers with an SSID or Wired Profile 162
In the CLI 163
Configuring 802.1X Authentication for a Network Profile 163
Configuring 802.1X Authentication for a Wireless Network Profile 164
In the Instant UI 164

In the CLI 164
Configuring 802.1X Authentication for Wired Profiles 164
In the Instant UI 165
In the CLI 165
Configuring MAC Authentication for a Network Profile 165
Configuring MAC Authentication for Wireless Network Profiles 165
In the Instant UI 165
In the CLI 166
Configuring MAC Authentication for Wired Profiles 166
In the Instant UI 166
In the CLI 167
Configuring MAC Authentication with 802.1X Authentication 167
Configuring MAC and 802.1X Authentication for a Wireless Network Profile 167
In the Instant UI 167
In the CLI 168
Configuring MAC and 802.1X Authentication for Wired Profiles 168
In the Instant UI 168
In the CLI 168
Configuring MAC Authentication with Captive Portal Authentication 169
Configuring MAC Authentication with Captive Portal Authentication 169
In the Instant UI 169
In the CLI 169
Configuring WISPr Authentication 170
In the Instant UI 170
In the CLI 170
Blacklisting Clients 171
Blacklisting Clients Manually 171
Adding a Client to the Blacklist 171
In the Instant UI 171
In the CLI 171
Blacklisting Users Dynamically 172
Authentication Failure Blacklisting 172

Session Firewall Based Blacklisting 172
Configuring Blacklist Duration 172
In the Instant UI 172
In the CLI 172
Uploading Certificates 173
Loading Certificates through Instant UI 173
Loading Certificates through Instant CLI 174
Loading Certificates through W-AirWave 174
Roles and Policies 176
Firewall Policies 176
Access Control List Rules 176
Configuring Access Rules for Network Services 177
In the Instant UI 177
In the CLI 178
Example 178
Configuring Network Address Translation Rules 179
Configuring a Source NAT Access Rule 179
In the Instant UI 179
In the CLI 179
Configuring Source-Based Routing 180
Configuring a Destination NAT Access Rule 180
In the Instant UI 180
In the CLI 180
Configuring ALG Protocols 181
In the Instant UI 181
In the CLI 181
Configuring Firewall Settings for Protection from ARP Attacks 181
In the Instant UI 182
In the CLI 182
Managing Inbound Traffic 183
Configuring Inbound Firewall Rules 183
In the Instant UI 183
In the CLI 185

Example 185
Configuring Management Subnets 185
In the Instant UI 185
In the CLI 186
Configuring Restricted Access to Corporate Network 186
In the Instant UI 186
In the CLI 186
Content Filtering 186
Enabling Content Filtering 187
Enabling Content Filtering for a Wireless Profile 187
In the Instant UI 187
In the CLI 187
Enabling Content Filtering for a Wired Profile 187
In the Instant UI 187
In the CLI 188
Configuring Enterprise Domains 188
In the Instant UI 188
In the CLI 188
Configuring URL Filtering Policies 188
In the Instant UI 188
In the CLI 189
Example 189
Configuring User Roles 190
Creating a User Role 190
In the Instant UI 190
In the CLI 190
Assigning Bandwidth Contracts to User Roles 190
In the Instant UI 191
In the CLI: 191
Configuring Machine and User Authentication Roles 191
In the Instant UI 191
In the CLI 192
Configuring Derivation Rules 192

Understanding Role Assignment Rule 192
RADIUS VSA Attributes 192
MAC-Address Attribute 192
Roles Based on Client Authentication 193
DHCP Option and DHCP Fingerprinting 193
Creating a Role Derivation Rule 193
In the Instant UI 193
In the CLI 194
Example 194
Understanding VLAN Assignment 194
Vendor Specific Attributes 195
VLAN Assignment Based on Derivation Rules 196
User Role 196
VLANs Created for an SSID 196
Configuring VLAN Derivation Rules 196
In the Instant UI 196
In the CLI 197
Example 198
Using Advanced Expressions in Role and VLAN Derivation Rules 198
Configuring a User Role for VLAN Derivation 199
Creating a User VLAN Role 199
In the Instant UI 199
In the CLI 199
Assigning User VLAN Roles to a Network Profile 200
In the Instant UI 200
In the CLI 200
DHCP Configuration 201
Configuring DHCP Scopes 201
Configuring Distributed DHCP Scopes 201
In the Instant UI 201
In the CLI 203
Configuring a Centralized DHCP Scope 204
In the Instant UI 204

In the CLI 205
Configuring Local and Local,L3 DHCP Scopes 206
In the Instant UI 206
In the CLI 207
Configuring the Default DHCP Scope for Client IP Assignment 208
In the Instant UI 208
In the CLI 209
VPN Configuration 210
Understanding VPN Features 210
Configuring a Tunnel from a W-IAP to Dell Networking W-Series Mobility Controller 210
Configuring an IPSec Tunnel 210
In the Instant UI 210
In the CLI 211
Example 212
Enabling Automatic Configuration of GRE Tunnel 212
In the Instant UI 212
In the CLI 214
Manually Configuring a GRE Tunnel 214
In the Instant UI 214
In the CLI 215
Configuring an L2TPv3 Tunnel 215
In the Instant UI 216
In the CLI 218
Example 218
Configuring Routing Profiles 221
In the Instant UI 221
In the CLI 222
IAP-VPN Deployment 223
Understanding IAP-VPN Architecture 223
IAP-VPN Scalability Limits 223
IAP-VPN Forwarding Modes 224
Local or NAT Mode 224

L2 Switching Mode 224
Distributed L2 Mode 224
Centralized L2 Mode 224
L3 Routing Mode 225
Distributed L3 mode 225
Centralized L3 Mode 225
Configuring W-IAP and Controller for IAP-VPN Operations 225
Configuring a W-IAP network for IAP-VPN operations 225
Defining the VPN host settings 225
Configuring Routing Profiles 226
Configuring DHCP Profiles 226
Configuring an SSID or Wired Port 226
Enabling Dynamic RADIUS Proxy 227
Configuring Enterprise Domains 227
Configuring a Controller for IAP-VPN Operations 227
OSPF Configuration 227
VPN Configuration 229
Whitelist Database Configuration 229
VPN Local Pool Configuration 230
Role Assignment for the Authenticated W-IAPs 230
VPN Profile Configuration 230
Branch-ID Allocation 230
Branch Status Verification 230
Example 230
Adaptive Radio Management 232
ARM Overview 232
Channel or Power Assignment 232
Voice Aware Scanning 232
Load Aware Scanning 232
Monitoring the Network with ARM 232
ARM Metrics 232
Configuring ARM Features on a W-IAP 233
Band Steering 233

In the Instant UI 233
In the CLI 233
Airtime Fairness Mode 233
In the Instant UI 234
In the CLI 234
Client Match 234
In the Instant UI 235
In the CLI 236
Access Point Control 236
In the Instant UI 236
In the CLI 237
Verifying ARM Configuration 237
Configuring Radio Settings for a W-IAP 238
In the Instant UI 238
In the CLI 239
Deep Packet Inspection and Application Visibility 241
Deep Packet Inspection 241
Enabling Application Visibility 241
In the Instant UI 241
In the CLI 241
Application Visibility 242
Application Category Charts 242
Application Charts 243
Web Categories Charts 245
Web Reputation Charts 245
Configuring Access Rules for Application and Application Categories 246
In the Instant UI 246
In the CLI 248
Example 249
Configuring Web Policy Enforcement 249
In the Instant UI 249
In the CLI 250

Example 250
Voice and Video 251
Wi-Fi Multimedia Traffic Management 251
Configuring WMM for Wireless Clients 251
In the Instant UI 252
In the CLI 252
Configuring WMM-DSCP Mapping 252
In the Instant UI 253
In the CLI 253
QoS for Microsoft Office OCS and Apple Facetime 253
Microsoft OCS 253
Apple Facetime 253
Services 255
AirGroup Configuration 255
Multicast DNS and Bonjour® Services 256
DLNA UPnP Support 257
AirGroup Features 258
AirGroup Services 259
AirGroup Components 260
CPPM and ClearPass Guest Features 260
Configuring AirGroup and AirGroup Services on a W-IAP 261
In the Instant UI 261
In the CLI 262
Configuring AirGroup and CPPM interface in Instant 263
Creating a RADIUS Server 263
Assign a Server to AirGroup 263
Configure CPPM to Enforce Registration 263
Change of Authorization (CoA) 263
Configuring a W-IAP for RTLS Support 263
In the Instant UI 263
In the CLI 264
Configuring a W-IAP for Analytics and Location Engine Support 265

ALE with Instant 265
Enabling ALE Support on a W-IAP 265
In the Instant UI 265
In the CLI 266
Verifying ALE Configuration on a W-IAP 266
Configuring OpenDNS Credentials 266
In the Instant UI 266
In the CLI 267
Integrating a W-IAP with Palo Alto Networks Firewall 267
Integration with Instant 267
Configuring a W-IAP for PAN integration 267
In the Instant UI 267
In the CLI 268
Integrating a W-IAP with an XML API interface 268
Integration with Instant 269
Configuring a W-IAP for XML API integration 269
In the Instant UI 269
In the CLI 269
CALEA Integration and Lawful Intercept Compliance 270
CALEA Server Integration 270
Traffic Flow from IAP to CALEA Server 270
Traffic Flow from IAP to CALEA Server through VPN 271
Client Traffic Replication 271
Configuring a W-IAP for CALEA Integration 271
Creating a CALEA Profile 272
In the Instant UI 272
In the CLI 272
Creating an Access Rule for CALEA 272
In the Instant UI 272
In the CLI 273
Verifying the configuration 273
Example 273

W-IAP Management and Monitoring 275
Managing a W-IAP from W-AirWave 275
Image Management 275
W-IAP and Client Monitoring 275
Template-based Configuration 275
Trending Reports 276
Intrusion Detection System 276
Wireless Intrusion Detection System (WIDS) Event Reporting to W-AirWave 276
RF Visualization Support for Instant 276
PSK-based and Certificate-based Authentication 277
Configurable Port for W-IAP and W-AirWave Management Server Communication 277
Configuring Organization String 277
Shared Key 278
Configuring W-AirWave Information 278
In the Instant UI 278
In the CLI 278
Configuring for W-AirWave Discovery through DHCP 279
Standard DHCP option 60 and 43 on Windows Server 2008 279
Alternate Method for Defining Vendor-Specific DHCP Options 283
Uplink Configuration 285
Uplink Interfaces 285
Ethernet Uplink 285
Configuring PPPoE Uplink Profile 286
In the Instant UI 286
In the CLI 287
Cellular Uplink 287
Configuring Cellular Uplink Profiles 290
In the Instant UI 290
In the CLI 290
Wi-Fi Uplink 291
Configuring a Wi-Fi Uplink Profile 291
Uplink Preferences and Switching 292

Enforcing Uplinks ... 292
In the Instant UI ... 292
In the CLI ... 293
Setting an Uplink Priority ... 293
In the Instant UI ... 293
In the CLI ... 293
Enabling Uplink Preemption ... 293
In the Instant UI ... 293
In the CLI ... 293
Switching Uplinks Based on VPN and Internet Availability ... 294
Switching Uplinks Based on VPN Status ... 294
Switching Uplinks Based on Internet Availability ... 294
In the Instant UI ... 294
In the CLI ... 295
Viewing Uplink Status and Configuration ... 295
Intrusion Detection ... 296
Detecting and Classifying Rogue APs ... 296
OS Fingerprinting ... 296
Configuring Wireless Intrusion Protection and Detection Levels ... 297
Containment Methods ... 301
Configuring IDS Using CLI ... 301
Mesh W-IAP Configuration ... 303
Mesh Network Overview ... 303
Mesh W-IAPs ... 303
Mesh Portals ... 303
Mesh Points ... 304
Setting up Instant Mesh Network ... 304
Configuring Wired Bridging on Ethernet 0 for Mesh Point ... 304
In the Instant UI ... 305
In the CLI ... 305
Mobility and Client Management ... 306
Layer-3 Mobility Overview ... 306
Configuring L3-Mobility ... 307

Home Agent Load Balancing 307
Configuring a Mobility Domain for Instant 307
In the Instant UI 307
In the CLI 308
Spectrum Monitor 309
Understanding Spectrum Data 309
Device List 309
Non Wi-Fi Interferers 310
Channel Details 312
Channel Metrics 313
Spectrum Alerts 314
Configuring Spectrum Monitors and Hybrid W-IAPs 314
Converting a W-IAP to a Hybrid W-IAP 314
In the Instant UI 315
In the CLI 315
Converting a W-IAP to a Spectrum Monitor 315
In the Instant UI 315
In the CLI 315
W-IAP Maintenance 317
Upgrading a W-IAP 317
Upgrading a W-IAP and Image Server 317
Image Management Using W-AirWave 317
Image Management Using Cloud Server 317
Configuring HTTP Proxy on a W-IAP 317
In the Instant UI 317
In the CLI 318
Upgrading a W-IAP Using Automatic Image Check 318
Upgrading to a New Version Manually 319
Upgrading an Image Using CLI 319
Backing up and Restoring W-IAP Configuration Data 319
Viewing Current Configuration 319
Backing up Configuration Data 320

Restoring Configuration 320
Converting a W-IAP to a Remote AP and Campus AP 320
Regulatory Domain Restrictions for W-IAP to RAP or CAP Conversion 320
Converting a W-IAP to a Remote AP 322
Converting a W-IAP to a Campus AP 323
Converting a W-IAP to Standalone Mode 324
Converting a W-IAP using CLI 325
Resetting a Remote AP or Campus AP to a W-IAP 325
Rebooting the W-IAP 325
Monitoring Devices and Logs 327
Configuring SNMP 327
SNMP Parameters for W-IAP 327
Configuring SNMP 328
Creating community strings for SNMPv1 and SNMPv2 Using Instant UI 328
Creating community strings for SNMPv3 Using Instant UI 328
Configuring SNMP Community Strings in the CLI 329
Configuring SNMP Traps 330
In the Instant UI 330
In the CLI 330
Configuring a Syslog Server 330
In the Instant UI 330
In the CLI 332
Configuring TFTP Dump Server 332
In the Instant UI 332
In the CLI 332
Running Debug Commands from the UI 333
Support Commands 333
Hotspot Profiles 338
Understanding Hotspot Profiles 338
Generic Advertisement Service (GAS) 338
Access Network Query Protocol (ANQP) 339
Hotspot 2.0 Query Protocol (H2QP) 339

Information Elements (IEs) and Management Frames 339
NAI Realm List 339
Configuring Hotspot Profiles 339
Creating Advertisement Profiles for Hotspot Configuration 340
Configuring an NAI Realm Profile 340
Configuring a Venue Name Profile 342
Configuring a Network Authentication Profile 343
Configuring a Roaming Consortium Profile 344
Configuring a 3GPP Profile 344
Configuring an IP Address Availability Profile 344
Configuring a Domain Profile 344
Configuring an Operator-friendly Profile 345
Configuring a Connection Capability Profile 345
Configuring an Operating Class Profile 345
Configuring a WAN Metrics Profile 345
Creating a Hotspot Profile 346
Associating an Advertisement Profile to a Hotspot Profile 348
Creating a WLAN SSID and Associating Hotspot Profile 349
Sample Configuration 349
ClearPass Guest Setup 352
Testing 355
Troubleshooting 355
IAP-VPN Deployment Scenarios 356
Scenario 1 - IPSec: Single Datacenter Deployment with No Redundancy 357
Topology 357
AP Configuration 357
AP Connected Switch Configuration 359
Datacenter Configuration 359
Scenario 2 - IPSec: Single Datacenter with Multiple Controllers for Redundancy 360
Topology 360
AP Configuration 361
AP Connected Switch Configuration 363

Datacenter Configuration 363
Scenario 3 - IPSec: Multiple Datacenter Deployment with Primary and Backup Controllers for Redundancy 364
Topology 364
AP Configuration 365
AP Connected Switch Configuration 368
Datacenter Configuration 368
Scenario 4 - GRE: Single Datacenter Deployment with No Redundancy 369
Topology 369
AP Configuration 369
AP Connected Switch Configuration 371
Datacenter Configuration 371
Terminology 373
Acronyms and Abbreviations 373
Glossary 374

This User Guide describes the features supported by Dell Networking W-Series Instant Access Point (W-IAP) and provides detailed instructions for setting up and configuring the Instant network.

Intended Audience

This guide is intended for customers who configure and use W-IAPs.

Related Documents

In addition to this document, the Dell W-IAP product documentation includes the following:

- *Dell Networking W-Series Instant Access Point Installation Guides*
- *Dell Networking W-Series Instant 6.4.0.2-4.1 Quick Start Guide*
- *Dell Networking W-Series Instant 6.4.0.2-4.1 CLI Reference Guide*
- *Dell Networking W-Series Instant 6.4.0.2-4.1 MIB Reference Guide*
- *Dell Networking W-Series Instant 6.4.0.2-4.1 Syslog Messages Reference Guide*
- *Dell Networking W-Series Instant 6.4.0.2-4.1 Release Notes*

Conventions

The following conventions are used throughout this manual to emphasize important concepts:

Table 1: *Typographical Conventions*

Type Style	Description
Italics	This style is used to emphasize important terms and to mark the titles of books.
`System items`	This fixed-width font depicts the following: • Sample screen output • System prompts • Filenames, software devices, and specific commands when mentioned in the text.
`Commands`	In the command examples, this style depicts the keywords that must be typed exactly as shown.
<Arguments>	In the command examples, italicized text within angle brackets represents items that you should replace with information appropriate to your specific situation. For example: `# send <text message>` In this example, you would type “send” at the system prompt exactly as shown, followed by the text of the message you wish to send. Do not type the angle brackets.
`[Optional]`	Command examples enclosed in brackets are optional. Do not type the brackets.
`{Item A | Item B}`	In the command examples, items within curled braces and separated by a vertical bar represent the available choices. Enter only one choice. Do not type the braces or bars.

The following informational icons are used throughout this guide:

Indicates helpful suggestions, pertinent information, and important things to remember.

Indicates a risk of damage to your hardware or loss of data.

Indicates a risk of personal injury or death.

Contacting Dell

Table 2: *Support Information*

Support	
Main Website	**dell.com**
Contact Information	**dell.com/contactdell**
Support Website	**dell.com/support**
Documentation Website	**dell.com/support/manuals**

This chapter provides the following information:

- Instant Overview
- What is New in Instant 6.4.0.2-4.1

Instant Overview

Instant virtualizes Dell Networking W-Series Mobility Controller capabilities on 802.11 access points (APs), creating a feature-rich enterprise-grade wireless LAN (WLAN) that combines affordability and configuration simplicity.

Instant is a simple, easy to deploy turn-key WLAN solution consisting of one or more APs. An Ethernet port with routable connectivity to the Internet or a self-enclosed network is used for deploying an Instant Wireless Network. A Dell Networking W-Series Instant Access Point (W-IAP) can be installed at a single site or deployed across multiple geographically-dispersed locations. Designed specifically for easy deployment, and proactive management of networks, Instant is ideal for small customers or remote locations without any on-site IT administrator.

Instant consists of a W-IAP and a Virtual Controller. The Virtual Controller resides within one of the APs. In a Instant deployment scenario, only the first W-IAP needs to be configured. After the first W-IAP is configured, the other W-IAPs inherit all the required configuration information from the Virtual Controller. Instant continually monitors the network to determine the W-IAP that should function as the Virtual Controller at any time, and the Virtual Controller will move from one W-IAP to another as necessary without impacting network performance.

Supported Devices

The following devices are supported in Instant 6.4.0.2-4.1:

- W-IAP103
- W-IAP104/ 105
- W-IAP114/115
- W-IAP134/135
- IAP-175P/175AC
- W-IAP3WN/3WNP
- W-IAP108/109
- W-IAP155/155P
- W-IAP224/225
- W-IAP274/275

As of Instant 4.1 release, it is recommended that networks with more than 128 APs should be designed as multiple, smaller virtual-controller networks with Layer-3 mobility enabled between them.

The following table provides the variants supported for each IAP model:

Table 3: *Supported W-IAP Variants*

W-IAP Model (Reg Domain)	W-IAP-###-US (US only)	W-IAP-###-JP (Japan only)	W-IAP-###-RW (Worldwide except US)	W-IAP-### (Worldwide except US and Japan)
W-IAP103	Yes	No	Yes	No
W-IAP104/ 105	Yes	Yes	No	Yes
W-IAP114/115	Yes	No	Yes	No
W-IAP134/135	Yes	Yes	No	Yes
IAP-175P/175AC	Yes	Yes	No	Yes
W-IAP3WN/3WNP	Yes	Yes	No	Yes
W-IAP108/109	Yes	Yes	No	Yes
W-IAP155/155P	Yes	Yes	No	Yes
W-IAP224/225	Yes	No	Yes	No
W-IAP274/275	Yes	No	Yes	No

For information on regulatory domains and the list of countries supported by the W-IAP-RW type, see Country Code on page 38.

Instant UI

The Instant User Interface (UI) provides a standard Web-based interface that allows you to configure and monitor a Wi-Fi network. Instant is accessible through a standard Web browser from a remote management console or workstation and can be launched using the following browsers:

- Microsoft Internet Explorer 10 or lower
- Apple Safari 6.0 or later
- Google Chrome 23.0.1271.95 or later
- Mozilla Firefox 17.0 or later

If the Instant UI is launched through an unsupported browser, a warning message is displayed along with a list of recommended browsers. However, the users are allowed to login using the **Continue login** link on the Login page.

To view the Instant UI, ensure that the JavaScript is enabled on the Web browser.

The Instant UI logs out automatically if the window is inactive for 15 minutes.

Instant CLI

The Instant Command Line Interface (CLI) is a text-based interface accessible through a Secure Shell (SSH) session.

SSH access requires that you configure an IP address and a default gateway on the W-IAP and connect the W-IAP to your network. This is typically performed when the Instant network on a W-IAP is set up.

What is New in Instant 6.4.0.2-4.1

The following features are added in the Instant 6.4.0.2-4.1 release:

Table 4: *New Features in 6.4.0.2-4.1*

Feature	Description
Support for AppRF	In this release, Instant supports AppRF comprising of two feature sets: On-board Deep Packet Inspection (DPI) and Web Policy Enforcement (WPE). As part of the AppRF feature support, Instant supports the following : • Access control based on application and application categories • Access control based on web categories and security ratings assigned to the websites
Support for new 4G modems	Instant now supports the following 4G modems: • Netgear Aircard 341u • Pantech UML295 • Franklin Wireless u770 • Huawei 3276s-150
AirGroup Enhancements	Instant supports Universal Plug and Play (UPnP) and DLNA (Digital Living Network Alliance) enabled devices. DLNA is a network standard derived from UPnP, which enables devices to discover the services available in a network.
DSCP Mapping for WMM Access Categories	Instant supports customization of Wi-Fi Multimedia to DSCP mapping configuration for upstream and downstream traffic.
Fast roaming enhancements	Instant supports 802.11k (Radio Resource Management) and 802.11v (BSS Transition Management) standards to improve Quality of Service (QoS) and seamless connectivity.
Authentication survivability with EAP-TLS	Instant supports the authentication survivability feature with the EAP-TLS authentication protocol. The authentication survivability feature supports a survivable authentication framework against the remote link failure when working with the external authentication servers.
Support for AP zone configuration	You can configure zone settings on a W-IAP and an SSID, so that the SSID is created on s specific W-IAP in the cluster.
Configurable port for communication between W-IAP and W-AirWave management server communication	You can customize the port number of the W-AirWave management server through the **server_host:server_port** format, for example, **amp.aruba.com:4343**.
Client match visualization	The Instant UI provides a graphical representation of the client distribution on an AP, the RSSI details, and the channel availability and utilization metrics.
Console access to W-IAP	In this release, you can allow or restrict access to a W-IAP console through the serial port. By default, the console access to an IAP is enabled.
Backup RADIUS server with EAP termination	Instant supports the configuration of the primary and backup RADIUS servers in an enterprise WLAN SSID that has EAP termination enabled.
Support for TACACS+ Server	In this release, a new external server type called TACACS+ Server is added to support authentication and accounting privileges for management users.

Table 4: *New Features in 6.4.0.2-4.1*

Feature	Description
XML API Integration	The Instant UI allows users to integrate an XML API Interface with a W-IAP. The users can use the XML API interface to add, delete, authenticate, or query a user or a client.
Support for inbound firewall rules configuration	You can configure firewall rules based on the source subnet for the inbound traffic coming through the uplink ports of a W-IAP.
Full tunnel support	For Centralized-L2 mode SSID, you can disable split-tunnel to tunnel all packets on the SSID through the VPN tunnel. This overrides any global routing profiles and sends all traffic from the client including DNS packets into the VPN tunnel.

Table 5: *New Hardware Platforms introduced in this release*

W-IAP Platform	Description
W-IAP270 Series	The W-IAP270 Series (W-IAP274 and W-IAP275) are environmentally hardened, outdoor rated, dual-radio IEEE 802.11ac wireless access points. These access points use MIMO (Multiple-in, Multiple-out) technology and other high-throughput mode techniques to deliver high-performance, 802.11ac 2.4 GHz and 5 GHz functionality while simultaneously supporting existing 802.11a/b/g/n wireless services. For more information about this product, visit **dell.com.**
W-IAP103	The W-IAP103 wireless access point supports the IEEE 802.11n standard for high-performance WLAN. This access point uses MIMO (Multiple-in, Multiple-out) technology and other high-throughput mode techniques to deliver high performance, 802.11n 2.4 GHz or 5 GHz functionality while simultaneously supporting existing 802.11a/b/g wireless services. For more information about this product, visit **dell.com**.

Check with your local Dell sales representative on device availability for your region.

This chapter describes the following procedures:

- Setting up Instant Network on page 35
- Logging in to the Instant UI on page 37
- Accessing the Instant CLI on page 41

Setting up Instant Network

Before installing a W-IAP:

- Ensure that you have an Ethernet cable of the required length to connect a W-IAP to the home router.
- Ensure that you have one of the following power sources:
  - IEEE 802.3af/at-compliant Power over Ethernet (PoE) source. The PoE source can be any power source equipment (PSE) switch or a midspan PSE device.
  - W-IAP power adapter kit.

Perform the following procedures to set up the Instant network:

1. Connecting a W-IAP on page 35
2. Assigning an IP address to the W-IAP on page 35
3. Connecting to a Provisioning Wi-Fi Network on page 36

Connecting a W-IAP

Based on the type of the power source used, perform one of the following steps to connect a W-IAP to the power source:

- PoE switch– Connect the ENET 0 port of the W-IAP to the appropriate port on the PoE switch.
- PoE midspan– Connect the ENET 0 port of the W-IAP to the appropriate port on the PoE midspan.
- AC to DC power adapter– Connect the 12V DC power jack socket to the AC to DC power adapter.

W-IAP155P supports PSE for 802.3at powered device (class 0-4) on one port (E1 or E2), or 802.3af powered DC IN (Power Socket) on two ports (E1 and E2).

Assigning an IP address to the W-IAP

The W-IAP needs an IP address for network connectivity. When you connect a W-IAP to a network, it receives an IP address from a DHCP server.

To obtain an IP address for a W-IAP:

1. Ensure that the DHCP service is enabled on the network.
2. Connect the ENET 0 port of W-IAP to a switch or router using an Ethernet cable.
3. Connect the W-IAP to a power source. The W-IAP receives an IP address provided by the switch or router.

If there is no DHCP service on the network, the W-IAP can be assigned a static IP address. If a static IP is not assigned, the W-IAP obtains an IP automatically within the 169.254 subnet.

Assigning a Static IP

To assign a static IP to a W-IAP:

1. Connect a terminal, PC, or workstation running a terminal emulation program to the **Console** port on the W-IAP.
2. Power on the W-IAP. An autoboot countdown prompt that allows you to interrupt the normal startup process and access **apboot** is displayed.
3. Click **Enter** before the timer expires. The W-IAP goes into the **apboot** mode.
4. In the **apboot** mode, use the following commands to assign a static IP to the W-IAP.

```
Hit <Enter> to stop autoboot: 0
apboot>
apboot> setenv ipaddr 192.0.2.0
apboot> setenv netmask 255.255.255.0
apboot> setenv gatewayip 192.0.2.2
apboot> save
Saving Environment to Flash...
Un-Protected 1 sectors
.done
Erased 1 sectors
Writing
```

5. Use the **`printenv`** command to view the configuration.

```
apboot> printenv
```

Connecting to a Provisioning Wi-Fi Network

The W-IAPs boot with factory default configuration and try to provision automatically. If the automatic provisioning is successful, the **instant** SSID will not be available. If W-AirWave and Activate are not reachable and the automatic provisioning fails, the **instant** SSID becomes available and the users can connect to a provisioning network by using the instant SSID.

To connect to a provisioning Wi-Fi network:

1. Ensure that the client is not connected to any wired network.
2. Connect a wireless enabled client to a provisioning Wi-Fi network: for example, **instant**.
3. If the Windows OS system is used:
   a. Click the wireless network connection icon in the system tray. The **Wireless Network Connection** window is displayed.
   b. Click on the **instant** network and then click **Connect**.
4. If the Mac OS system is used:
   a. Click the **AirPort** icon. A list of available Wi-Fi networks is displayed.
   b. Click on the **instant** network.

The **instant** SSIDs are broadcast in 2.4 GHz only.

W-IAP Cluster

W-IAPs in the same VLAN automatically find each other and form a single functioning network managed by a Virtual Controller.

Moving a W-IAP from one cluster to another requires a factory reset of the W-IAP.

Disabling the Provisioning Wi-Fi Network

The provisioning network is enabled by default. Instant provides the option to disable the provisioning network through the console port. Use this option only when you do not want the default SSID **instant** to be broadcast in your network.

To disable the provisioning network:

1. Connect a terminal or PC/workstation running a terminal emulation program to the **Console** port on the W-IAP.
2. Configure the terminal or terminal emulation program to use the following communication settings:

Table 6: *Terminal Communication Settings*

Baud Rate	Data Bits	Parity	Stop Bits	Flow Control
9600	8	None	1	None

3. Power on the W-IAP. An autoboot countdown prompt that allows you to interrupt the normal startup process and access apboot is displayed.
4. Click **Enter** before the timer expires. The W-IAP goes into the apboot mode through console.
5. In the apboot mode, use the following commands to disable the provisioning network:
   - `apboot> factory_reset`
   - `apboot> setenv disable_prov_ssid 1`
   - `apboot> saveenv`
   - `apboot> reset`

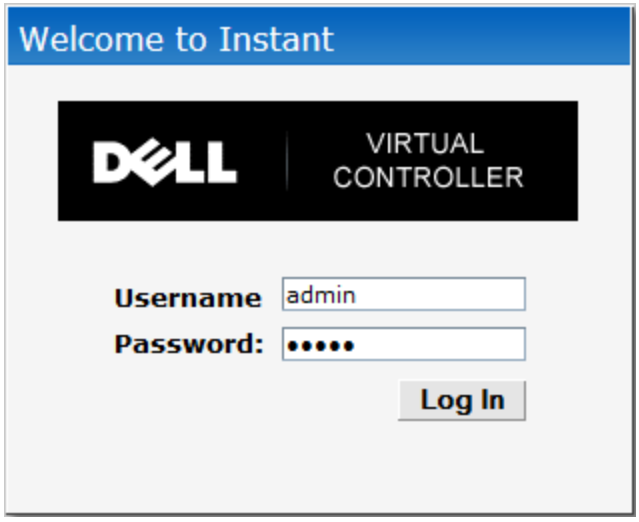
Logging in to the Instant UI

Launch a Web browser and enter **instant.dell-pcw.com**. In the login screen, enter the following credentials:

- Username– admin
- Password– admin

The following figure shows the **Login** screen:

Figure 1 *Login Screen*



When you use a provisioning Wi-Fi network to connect to the Internet, all browser requests are directed to the Instant UI. For example, if you enter **example.com** in the address field, you are directed to the Instant UI. You can change the default login credentials after the first login.

Regulatory Domains

The IEEE 802.11/b/g/n Wi-Fi networks operate in the 2.4 GHz spectrum and IEEE 802.11a/n operates in the 5.0 GHz spectrum. The spectrum is divided into channels. The 2.4 GHz spectrum is divided into 14 overlapping, staggered 20 MHz wireless carrier channels. These channels are spaced 5 MHz apart. The 5 GHz spectrum is divided into more channels. The channels that can be used in a particular country differ based on the regulations of that country.

The initial Wi-Fi setup requires you to specify the country code for the country in which the Instant operates. This configuration sets the regulatory domain for the radio frequencies that the W-IAPs use. Within the regulated transmission spectrum, a high-throughput 802.11ac, 802.11a, 802.11b/g, or 802.11n radio setting can be configured. The available 20 MHz, 40 MHz, or 80MHz channels are dependent on the specified country code.

You cannot change the country code for the W-IAPs in the restricted regulatory domains such as US or Japan for most of the W-IAP models. Improper country code assignments can disrupt wireless transmissions. Most countries impose penalties and sanctions on operators of wireless networks with devices set to improper country codes.

Country Code

The following table provides a list of supported country codes:

Table 7: *Country Codes List*

Code	Country Name
AE	United Arab Emirates
AR	Argentina
AT	Austria
AU	Australia
BG	Bulgaria
BH	Bahrain
BM	Bermuda
BO	Bolivia
BR	Brazil
CA	Canada
CH	Switzerland
CL	Chile
CN	China
CO	Colombia
CR	Costa Rica

Code	Country Name
CS	Serbia and Montenegro
CY	Cyprus
CZ	Czech Republic
DE	Germany
DK	Denmark
DO	Dominican Republic
DZ	Algeria
EC	Ecuador
EE	Estonia
EG	Egypt
ES	Spain
FI	Finland
FR	France
GB	United Kingdom
GR	Greece
GT	Guatemala
HK	Hong Kong
HN	Honduras
ID	Indonesia
IE	Ireland
IN	India
IS	Iceland
IT	Italy
JM	Jamaica
JO	Jordan
JP	Japan
KE	Kenya
KR	Republic of Korea (South Korea)

Code	Country Name
KW	Kuwait
LB	Lebanon
LI	Liechtenstein
LI	Liechtenstein
LK	Sri Lanka
LT	Lithuania
LU	Luxembourg
MA	Morocco
MU	Mauritius
MX	Mexico
NL	Netherlands
NO	Norway
NZ	New Zealand
OM	Oman
PA	Panama
PE	Peru
PH	Philippines
PK	Islamic Republic of Pakistan
PL	Poland
PR	Puerto Rico
PT	Portugal
QA	Qatar
RO	Romania
RU	Russia
SA	Saudi Arabia
SG	Singapore
SI	Slovenia
SK	Slovak Republic

Code	Country Name
SV	El Salvador
TH	Thailand
TN	Tunisia
TR	Turkey
TT	Trinidad and Tobago
TW	Taiwan
UA	Ukraine
US	United States
UY	Uruguay
VE	Venezuela
VN	Vietnam
ZA	South Africa

Specifying Country Code

NOTE

This procedure is applicable to the W-IAP-RW (Rest of World) variants only. Skip this step if you are installing W-IAP in the United States and Japan.

The **Country Code** window is displayed for the W-IAP-RW (Rest of World) variants when you log in to the UI for the first time. You can specify a country code by selecting an appropriate option from the **Please Specify the Country Code** drop-down list.

Figure 2 *Specifying a Country Code*

For the complete list of the country codes supported by the W-IAP-RW variant type, see Country Code on page 38.

Accessing the Instant CLI

Instant supports the use of Command Line Interface (CLI) for scripting purposes. When you make configuration changes on a master W-IAP in the CLI, all associated W-IAPs in the cluster inherit these changes and subsequently update their configurations. By default, you can access the CLI from the serial port or from an SSH session. You must explicitly enable Telnet access on the W-IAP to access the CLI through a Telnet session.

For information on enabling SSH and Telnet access to the W-IAP CLI, see Configuring Terminal Access on page 80.

Connecting to a CLI Session

On connecting to a CLI session, the system displays its host name followed by the login prompt. Use the administrator credentials to start a CLI session. For example:

```
(Instant AP)
User: admin
```

If the login is successful, the privileged command mode is enabled and a command prompt is displayed. For example:

```
(Instant AP)#
```

The privileged mode provides access to **show**, **clear**, **ping**, **traceroute**, and **commit** commands. The configuration commands are available in `config` mode. To move from privileged mode to the configuration mode, enter the following command at the command prompt:

```
(Instant AP)# configure terminal
```

The configure terminal command allows you to enter the basic configuration mode and the command prompt is displayed as follows:

```
(Instant AP)(config)#
```

The Instant CLI allows CLI scripting in several other sub-command modes to allow the users to configure individual interfaces, SSIDs, access rules, and security settings.

You can use the question mark (?) to view the commands available in a privileged mode, configuration mode, or sub-mode.

Although automatic completion is supported for some commands such as **configure terminal**, the complete **exit** and **end** commands must be entered at command prompt.

Applying Configuration Changes

Each command processed by the Virtual Controller is applied on all the slaves in a cluster. The changes configured in a CLI session are saved in the CLI context. The CLI does not support the configuration data exceeding the 4K buffer size in a CLI session. Therefore, it is recommended that you configure fewer changes at a time and apply the changes at regular intervals.

To apply and save the configuration changes at regular intervals, use the following command in the privileged mode:

```
(Instant AP)# commit apply
```

To apply the configuration changes to the cluster without saving the configuration, use the following command in the privileged mode:

```
(Instant AP)# commit apply no-save
```

To view the changes that are yet to be applied, use the following command in the privileged mode:

```
(Instant AP)# show uncommitted-config
```

To revert to the earlier configuration, use the following command in the privileged mode.

```
(Instant AP)# commit revert
```

Example:

```
(Instant AP)(config)# rf dot11a-radio-profile
(Instant AP)(RF dot11a Radio Profile)# beacon-interval 200
(Instant AP)(RF dot11a Radio Profile)# no legacy-mode
(Instant AP)(RF dot11a Radio Profile)# dot11h
(Instant AP)(RF dot11a Radio Profile)# interference-immunity 3
(Instant AP)(RF dot11a Radio Profile)# csa-count 2
(Instant AP)(RF dot11a Radio Profile)# spectrum-monitor
(Instant AP)(RF dot11a Radio Profile)# end
```

```
(Instant AP)# show uncommitted-config
   rf dot11a-radio-profile
   no legacy-mode
   beacon-interval 200
   no dot11h
   interference-immunity 3
   csa-count 1
   no spectrum-monitor

Instant Access Point# commit apply
```

Using Sequence Sensitive Commands

The Instant CLI does not support positioning or precedence of sequence-sensitive commands. Therefore, it is recommended that you remove the existing configuration before adding or modifying the configuration details for sequence-sensitive commands. You can either delete an existing profile or remove a specific configuration by using the **no…** commands.

The following table lists the sequence-sensitive commands and the corresponding **no** command to remove the configuration.

Table 8: *Sequence-Sensitive Commands*

Sequence-Sensitive Command	Corresponding no command
`opendns <username <password>`	`no opendns`
`rule <dest> <mask> <match> <protocol> <start-port> <end-port> {permit |deny | src-nat | dst-nat {<IP-address> <port>| <port>}}[<option1....option9>]`	`no rule <dest> <:mask> <match> <protocol> <start-port> <end-port> {permit | deny | src-nat | dst-nat}`
`mgmt-auth-server <auth-profile-name>`	`no mgmt-auth-server <auth-profile-name>`
`set-role <attribute>{{equals| not-equals| starts-with| ends-with| contains} <operator> <role>| value-of}`	`no set-role <attribute>{{equals| not-equals| starts-with| ends-with| contains} <operator>| value-of}` `no set-role`
`set-vlan <attribute>{{equals| not-equals| starts-with| ends-with| contains} <operator> <VLAN-ID>| value-of}`	`no set-vlan <attribute>{{equals| not-equals| starts-with| ends-with| contains} <operator>| value-of}` `no set-vlan`
`auth-server <name>`	`no auth-server <name>`

This chapter describes the following Instant UI elements:

- Login Screen
- Main Window

Login Screen

The Instant login page allows you to:

- Log in to the Instant UI.
- View Instant Network Connectivity summary
- View the Instant UI in a specific language

Logging into the Instant UI

To log in to the Instant UI, enter the following credentials:

- Username– admin
- Password– admin

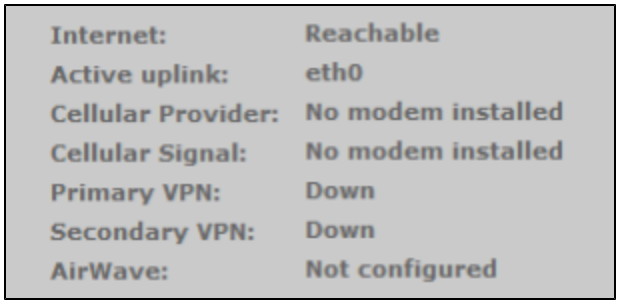
The Instant UI main window is displayed.

Viewing Connectivity Summary

The Login page also displays the connectivity status to the Instant network. The users can view a summary that indicates the status of the Internet availability, uplink, cellular modem and signal strength, VPN, and W-AirWave configuration details before logging in to the Instant UI.

The following figure shows the information displayed in the connectivity summary:

Figure 3 *Connectivity Summary*



NOTE

The Internet status is available only if the Internet failover feature (**System > Show advanced option > uplink > Internet failover**) is enabled.
The cellular provider and cellular strength information is only available when a 3G or 4G modem is in use.

Language

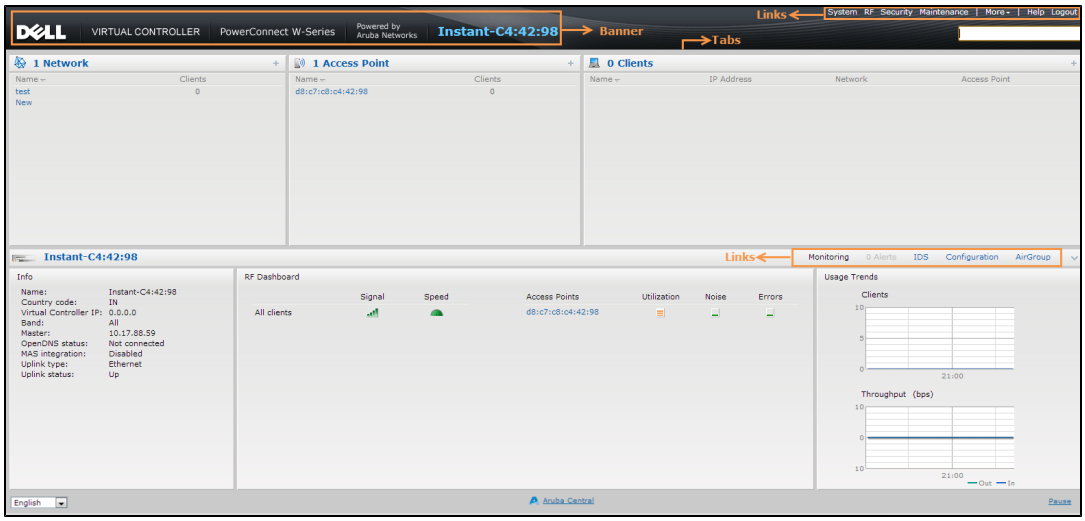
The **Language** drop-down lists the languages and allows users to select their preferred language before logging in to the Instant UI. A default language is selected based on the language preferences in the client desktop operating system or browser. If Instant cannot detect the language, then **English** is used as the default language.

You can also select the required language option from the **Languages** drop-down located at the bottom left corner of the Instant main window.

Main Window

On logging into Instant, the Instant UI Main Window is displayed. The following figure shows the Instant main window:

Figure 4 *Instant Main Window*



The main window consists of the following elements:

- Banner
- Search
- Tabs
- Links
- Views

Banner

The banner is a horizontal rectangle that appears at the top left corner of the Instant main window. It displays the company name, logo, and Virtual Controller's name.

Search

Administrators can search for a W-IAP, client, or a network in the **Search** text box. When you type a search text, the search function suggests matching keywords and allows you to automatically complete the search text entry.

Tabs

The Instant main window consists of the following tabs:

- Networks Tab– Provides information about the network profiles configured in the Instant network.
- Access Points Tab– Provides information about the W-IAPs configured in the Instant network.
- Clients Tab– Provides information about the clients in the Instant network.

Each tab appears in a compressed view by default. The number of networks, W-IAPs, or clients in the network precedes the tab names. The individual tabs can be expanded or collapsed by clicking on the tabs. The list items in each tab can be sorted by clicking the triangle icon next to the heading labels.

Networks Tab

This tab displays a list of Wi-Fi networks that are configured in the Instant network. The network names are displayed as links. The expanded view displays the following information about each WLAN SSID:

- **Name (SSID)** – Name of the network.
- **Clients** – Number of clients that are connected to the network.
- **Type** – Type of network type such as Employee, Guest, or Voice.
- **Band** – Band in which the network is broadcast: 2.4 GHz band, 5 GHz band, or both.
- **Authentication Method** – Authentication method required to connect to the network.
- **Key Management** – Authentication key type.
- **IP Assignment**– Source of IP address for the client.
- **Zone**–AP zone configured on the SSID.

To add a wireless network profile, click the **New** link in the **Networks** tab. To edit, click the **edit** link that is displayed on clicking the network name in the **Networks** tab. To delete a network, click on the link **x**.

For more information on the procedure to add or modify a wireless network, see Wireless Network Profiles on page 93.

Access Points Tab

If the Auto Join Mode feature is enabled, a list of enabled and active W-IAPs in the Instant network is displayed in the **Access Points** tab. The W-IAP names are displayed as links. If the Auto Join Mode feature is disabled, the **New** link is displayed. Click this link to add a new W-IAP to the network. If a W-IAP is configured and not active, its MAC Address is displayed in red.

The expanded view of the **Access Points** tab displays the following information about each W-IAP:

- **Name** – Name of the W-IAP. If the W-IAP functions as a master W-IAP in the network, the asterisk sign "*" is displayed next to the W-IAP.
- **IP Address** – IP address of the W-IAP.
- **Mode** – Mode of the W-IAP.
  - **Access** – In this mode, the AP serves clients and scans the home channel for spectrum analysis while monitoring channels for rogue APs in the background.
  - **Monitor** – In this mode, the AP acts as a dedicated Air Monitor (AM), scanning all channels for rogue APs and clients.
- **Spectrum**– When enabled, the AP functions as a dedicated full-spectrum RF monitor, scanning all channels to detect interference from neighboring APs or non-Wi-Fi devices such as microwaves and cordless phones. When Spectrum is enabled, the AP does not provide access services to clients.
- **Clients** – Number of clients that are currently associated to the W-IAP.
- **Type** – Model number of the W-IAP.
- **Zone**–AP zone.
- **Channel** – Channel on which the W-IAP is currently broadcast.
- **Power (dB)** – Maximum transmission EIRP of the radio.
- **Utilization (%)** – Percentage of time that the channel is utilized.
- **Noise (dBm)** – Noise floor of the channel.

An **edit** link is displayed on clicking the W-IAP name. For details about editing W-IAP settings see Customizing W-IAP Settings on page 84.

Clients Tab

This tab displays a list of clients that are connected to the Instant network. The client names are displayed as links. The expanded view displays the following information about each client:

- **Name** – User name of the client or guest users if available.
- **IP Address** – IP address of the client.
- **MAC Address** – MAC address of the client.
- **OS** – Operating system that runs on the client.
- **Network** – The network to which the client is connected.
- **Access Point** – W-IAP to which the client is connected.
- **Channel** – The client operating channel.
- **Type** – Type of the Wi-Fi client: A, G, AN, or GN.
- **Role** – Role assigned to the client.
- **Signal** – Current signal strength of the client, as detected by the AP.
- **Speed (mbps)** – Current speed at which data is transmitted. When the client is associated with an AP, it constantly negotiates the speed of data transfer. A value of 0 means that the AP has not heard from the client for some time.

Links

- The following links allow you to configure various features for the Instant network:
- New Version Available
- System
- RF
- Security
- Maintenance
- More
- Help
- Logout
- Monitoring
- Client Match
- AppRF
- Spectrum
- Alerts
- IDS
- Configuration
- AirGroup
- W-AirWave Setup
- Pause/Resume

Each of these links is explained in the subsequent sections.

New Version Available

This link is displayed in the top right corner of the Instant main window only if a new image version is available on the image server and W-AirWave is not configured. For more information about the **New version available** link and its functions, see Upgrading a W-IAP on page 317.

System

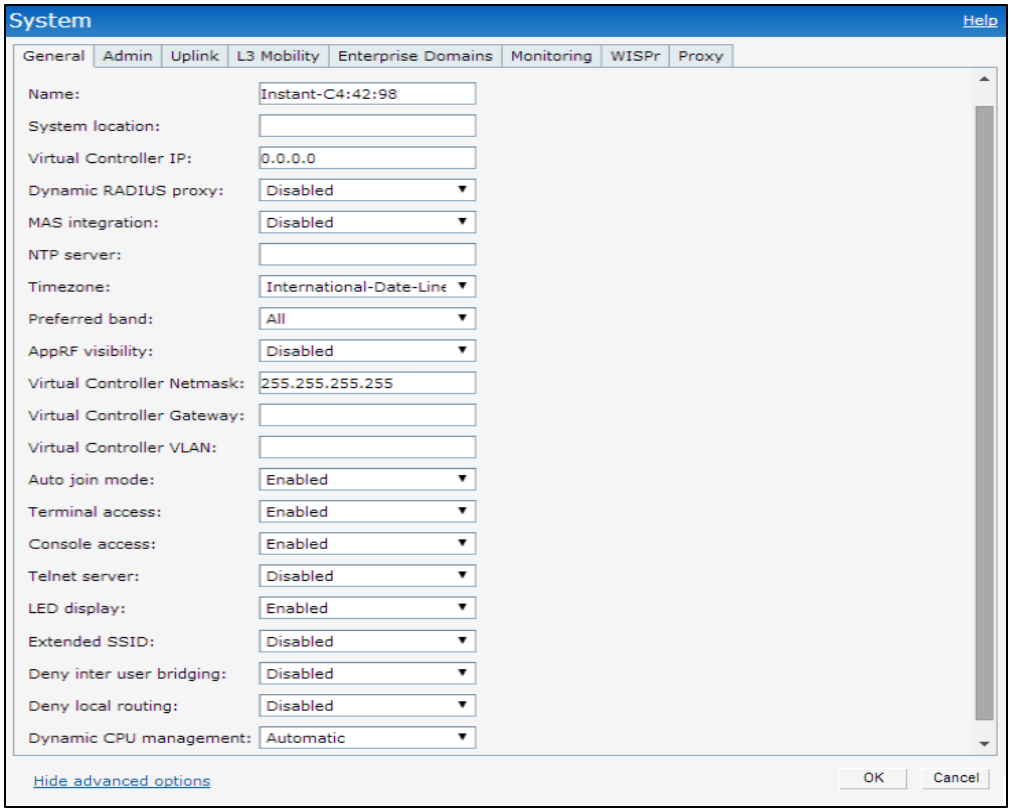
This link displays the **System** window. The **System** window consists of the following tabs:

Use the **Show/Hide Advanced** option at the bottom of the **System** window to view or hide the advanced options.

- **General**– Allows you to configure, view or edit the Name, IP address, NTP Server, and other W-IAP settings for the Virtual Controller. For more information on the basic and additional configuration settings that can be performed on this tab, see Basic Configuration Tasks on page 74 and Additional Configuration Tasks on page 78.
- **Admin** – Allows you to configure administrator credentials for access to the Virtual Controller Management User Interface. You can also configure W-AirWave in this tab. For more information on management interface and W-AirWave configuration, see Managing W-IAP Users on page 140 and Managing a W-IAP from W-AirWave on page 275 respectively.
- **Uplink** – Allows you to view or configure uplink settings. See Uplink Configuration on page 285 for more information.
- **L3 Mobility** – Allows you to view or configure the Layer-3 mobility settings. See Configuring L3-Mobility on page 307 for more information.
- **Enterprise Domains** – Allows you to view or configure the DNS domain names that are valid in the enterprise network. See Configuring Enterprise Domains on page 188 for more information.
- **Monitoring** – Allows you to view or configure the following details:
  - **Syslog** – Allows you to view or configure Syslog Server details for sending syslog messages to the external servers. See Configuring a Syslog Server on page 330 for more information.
  - **TFTP Dump** – Allows you to view or configure a TFTP dump server for core dump files. See Configuring TFTP Dump Server on page 332 for more information.
  - **SNMP** – Allows you to view or configure SNMP agent settings. See Configuring SNMP on page 327 for more information.
- **WISPr** – Allows you to view or configure the WISPr settings. See Configuring WISPr Authentication on page 170 for more information.
- **Proxy** – Allows you to configure HTTP proxy on a W-IAP. See Configuring HTTP Proxy on a W-IAP on page 317 for more information.

The following figure provides a view of the **System** window with the advanced options.

Figure 5 *System Window*



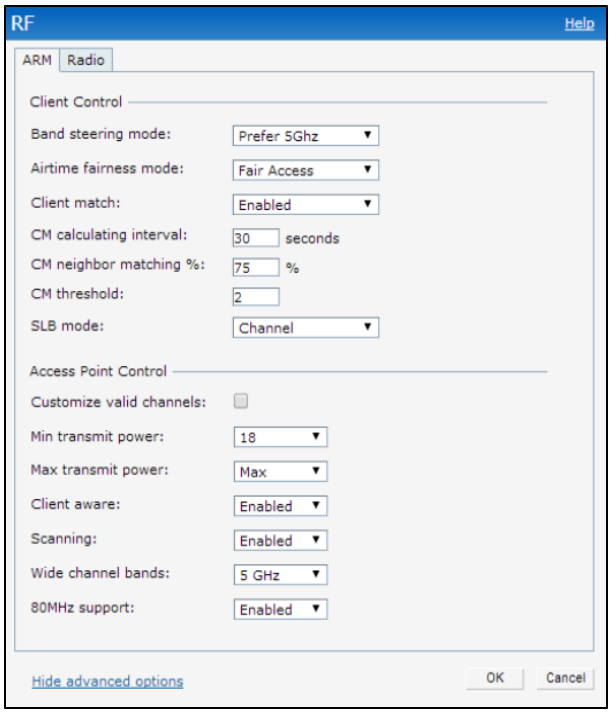
RF

The **RF** link displays a window for configuring Adaptive Radio Management (ARM) and Radio features.

- **ARM** – Allows you to view or configure channel and power settings for all the W-IAPs in the network. For information about ARM configuration, see ARM Overview on page 232.
- **Radio** – Allows you to view or configure radio settings for 2.4 GHz and the 5 GHz radio profiles. For information about Radio, see Configuring Radio Settings for a W-IAP on page 238.

The following figure provides a view of the **RF** window with the advanced options for ARM configuration:

Figure 6 *RF Window*



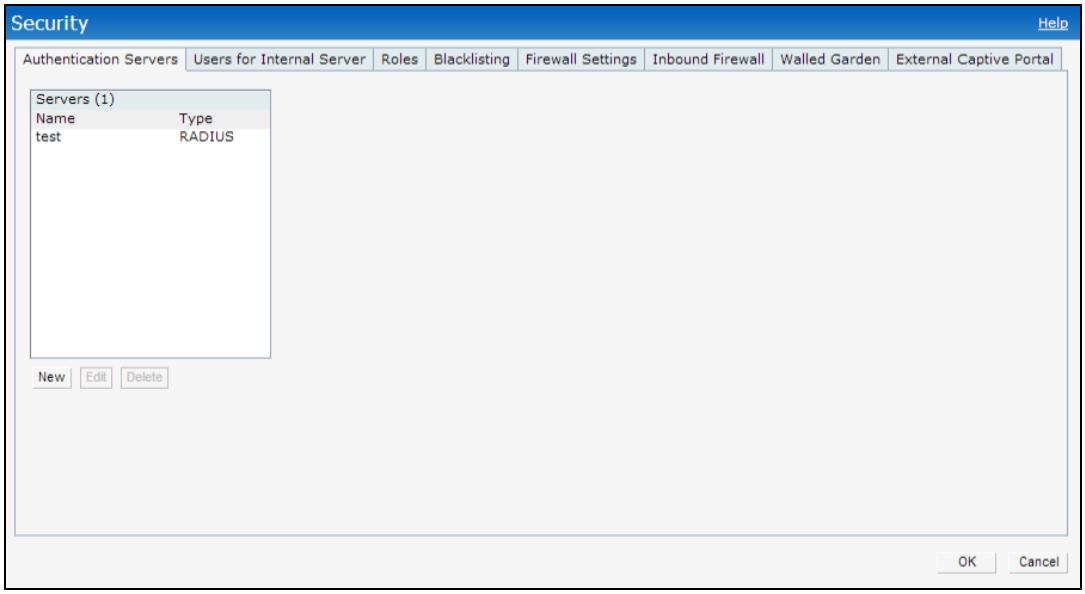
Security

The **Security** link displays a window with the following tabs:

- **Authentication Servers**– Use this tab to configure an external RADIUS server for a wireless network. For more information, see Configuring an External Server for Authentication on page 157.
- **Users for Internal Server**– Use this tab to populate the system's internal authentication server with users. This list is used by networks for which per-user authorization is specified using the Virtual Controller's internal authentication server. For more information about users, see Managing W-IAP Users on page 140.
- **Roles–** Use this tab to view the roles defined for all the Networks. The Access Rules part allows you to configure permissions for each role. For more information, see Configuring User Roles on page 190 and Configuring Access Rules for Network Services on page 177.
- **Blacklisting**– Use this tab to blacklist clients. For more information, see Blacklisting Clients on page 171.
- **Firewall Settings**– Use this tab to enable or disable Application Layer Gateway (ALG) supporting address and port translation for various protocols and to configure protection against wired attacks. For more information, see Configuring ALG Protocols on page 181 and Configuring Firewall Settings for Protection from ARP Attacks on page 181
- **Inbound Firewall**– Use this tab to enhance the inbound firewall by allowing configuration of inbound firewall rules, management subnets, and restricted corporate access through an uplink switch. For more information, see Managing Inbound Traffic on page 183.
- **Walled Garden**–Use this window to allow or prevent access to a selected list of websites. For more information, see Configuring Walled Garden Access on page 138.
- **External Captive Portal**– Use this window to configure external captive portal profiles. For more information, see Configuring External Captive Portal for a Guest Network on page 129.

The following figure shows the default view of the **Security** window:

Figure 7 *Security Window - Default View*



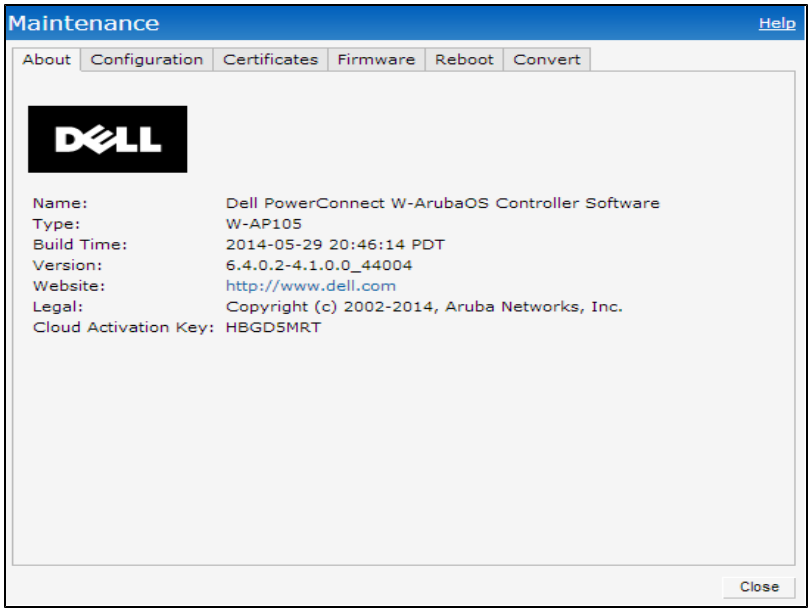
Maintenance

The **Maintenance** link displays a window that allows you to maintain the Wi-Fi network. The **Maintenance** window consists of the following tabs:

- **About**–Displays the name of the product, build time, W-IAP model name, the Instant version, website address of Dell, and Copyright information.
- **Configuration**– Displays the following details:
  - **Current Configuration** – Displays the current configuration details.
  - **Clear Configuration** –Allows you to clear the current configuration details of the network.
  - **Backup Configuration** – Allows you to back up local configuration details. The backed up configuration data is saved in the file named **instant.cfg**.
  - **Restore Configuration** – Allows you to restore the backed up configuration. The W-IAP must be rebooted after restoring the configuration for the changes to affect.
- **Certificates** – Displays information about the certificates installed on the W-IAP. You can also upload new certificates and set a passphrase for the certificates. For more information, see Uploading Certificates on page 173.
- **Firmware** – Displays the current firmware version and provides various options to upgrade to a new firmware version. For more information, see Upgrading a W-IAP on page 317.
- **Reboot** – Displays the W-IAPs in the network and provides an option to reboot the required access point or all access points. For more information, see Upgrading a W-IAP on page 317.
- **Convert** – Provides an option to convert a W-IAP to a mobility controller managed Remote AP or Campus AP, or to the default Virtual Controller mode. For more information, see Converting a W-IAP to a Remote AP and Campus AP on page 320.

The following figure shows the default view of the **Maintenance** window:

Figure 8 *Maintenance Window - Default View*



More

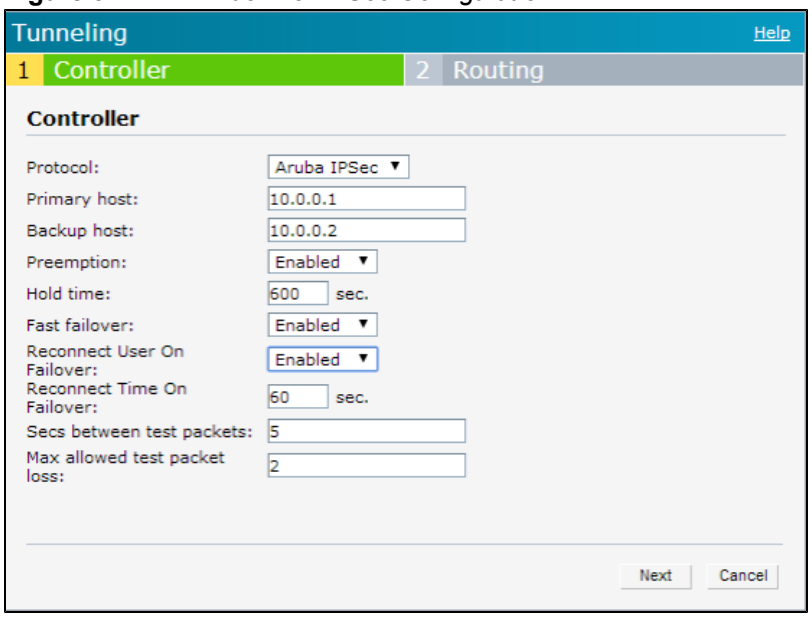
The **More** link allows you to select the following options:

- VPN
- IDS
- Wired
- Services
- DHCP Server
- Support

VPN

The **VPN** window allows you to define communication settings with a remote Controller. See VPN Configuration on page 210 for more information. The following figure shows an example of the IPSec configuration options available in the **VPN** window:

Figure 9 *VPN window for IPSec Configuration*



IDS

The IDS window allows you to configure wireless intrusion detection and protection levels. The following figures show the **IDS** window:

Figure 10 *IDS Window: Intrusion Detection*

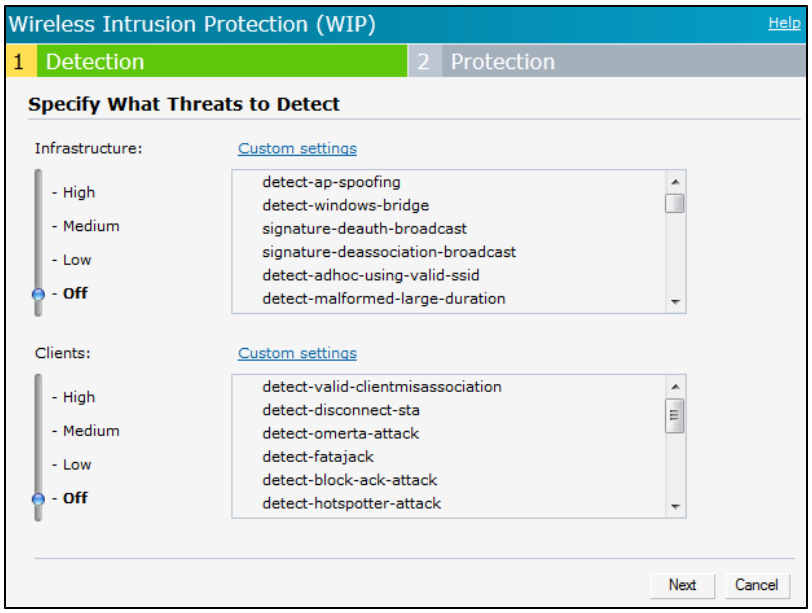
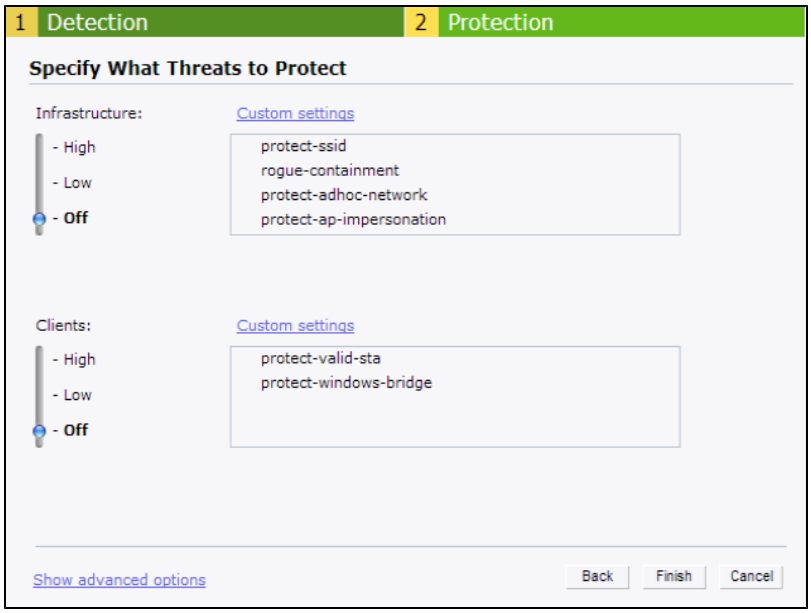


Figure 11 *IDS Window: Intrusion Protection*

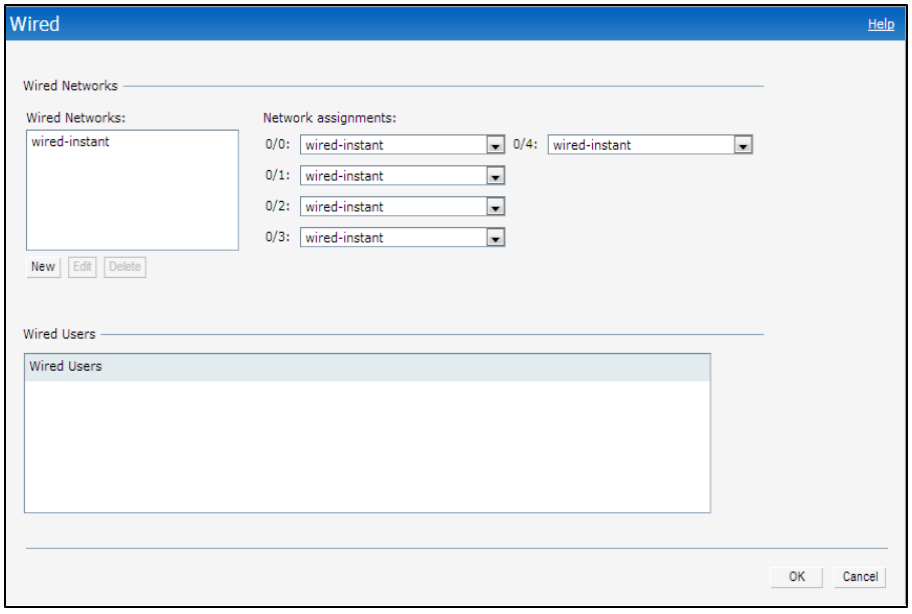


For more information on wireless intrusion detection and protection, see Detecting and Classifying Rogue APs on page 296.

Wired

The **Wired** window allows you to configure a wired network profile. See Wired Profiles on page 112 for more information. The following figure shows the **Wired** window:

Figure 12 *Wired Window*



Services

The **Services** window allows you to configure services such as AirGroup, RTLS, and OpenDNS. The Services window consists of the following tabs:

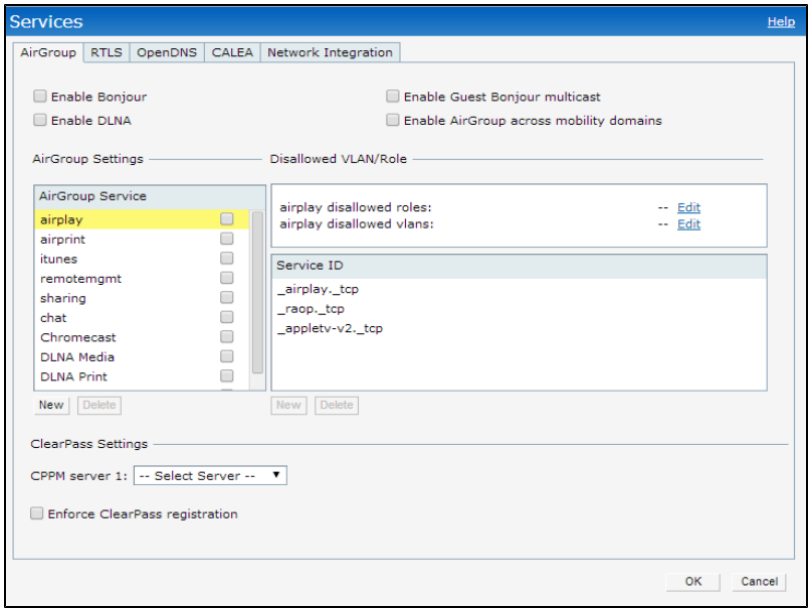
- **AirGroup** – Allows you to configure the AirGroup and AirGroup services. For more information, see AirGroup Configuration on page 255.

- **RTLS** – Allows you to integrate W-AirWave Management platform or third-party Real Time Location Server such as Aeroscout Real Time Location Server with Instant. For more information, see Configuring a W-IAP for RTLS Support on page 263.

  The RTLS tab also allows you to integrate W-IAP with the Analytics and Location Engine (ALE). For more information about configuring a W-IAP for ALE integration, see Configuring a W-IAP for Analytics and Location Engine Support on page 265.
- **OpenDNS**– Allows you to configure support for OpenDNS business solutions, which require an OpenDNS (opendns.com) account. The OpenDNS credentials are used by Instant and W-AirWave to filter content at the enterprise level. For more information, see Configuring OpenDNS Credentials on page 266.
- **CALEA**–Allows you configure support for Communications Assistance for Law Enforcement Act (CALEA) server integration, thereby ensuring compliance with Lawful Intercept and CALEA specifications. For more information, see CALEA Integration and Lawful Intercept Compliance on page 270.
- **Network Integration**–Allows you to configure a W-IAP for integration with Palo Alto Networks (PAN) Firewall and XML API server. For more information about W-IAP integration with PAN, see Integrating a W-IAP with Palo Alto Networks Firewall on page 267and Integrating a W-IAP with an XML API interface on page 268.

The following figure shows the default view of the **Services** window:

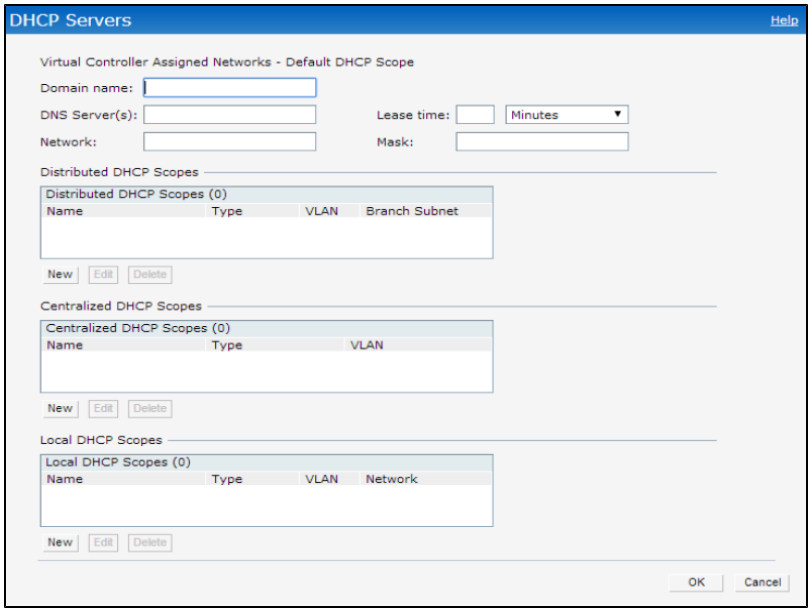
Figure 13 *Services Window: Default View*



DHCP Server

The DHCP Servers window allows you to configure various DHCP modes. The following figure shows the contents of the **DHCP Servers** window:

Figure 14 *DHCP Servers Window*



For more information, see DHCP Configuration on page 201.

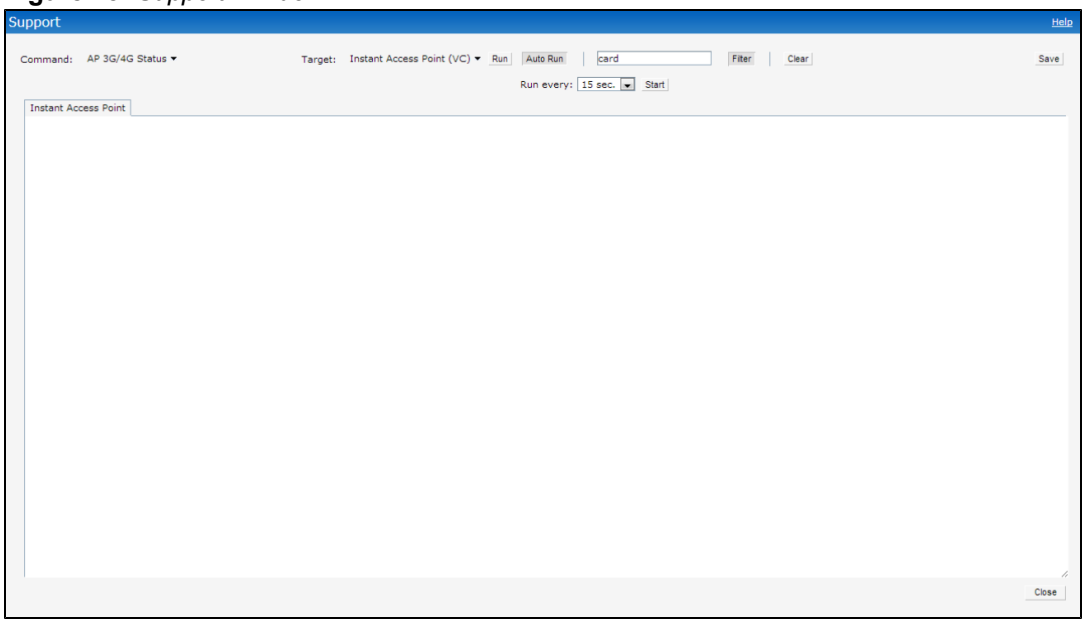
Support

The **Support** consists of the following fields:

- **Command**– Allows you to select a support command for execution.
- **Target**–Displays a list of W-IAPs in the network.
- **Run**– Allows you to execute the selected command for a specific W-IAP or all W-IAPs and view logs.
- **Auto Run**– Allows you to configure a schedule for automatic execution of a support command for a specific W-IAP or all W-IAPs.
- **Filter**–Allows you to filter the contents of a command output.
- **Clear**–Clears the command output displayed after a command is executed.
- **Save**– Allows you to save the support command logs as an HTML or text file.

For more information on support commands, see Running Debug Commands from the UI on page 333. The following figure shows the **Support** window:

Figure 15 *Support Window*



Help

The **Help** link allows you to view a short description or definition of selected terms and fields in the UI windows or dialogs.

To activate the context-sensitive help:

1. Click the **Help** link at the top right corner of Instant main window.
2. Click any text or term displayed in green italics to view its description or definition.
3. To disable the help mode, click **Done**.

Logout

The **Logout** link allows you to log out of the Instant UI.

Monitoring

The **Monitoring** link displays the Monitoring pane for the Instant network. Use the down arrow located to the right side of these links to compress or expand the monitoring pane.

The monitoring pane consists of the following sections:

- Info
- RF Dashboard
- RF Trends
- Usage Trends
- Mobility Trail

Info

The **Info** section displays the configuration information of the Virtual Controller by default. On selecting the Network View tab, the monitoring pane displays configuration information of the selected network. Similarly in the Access Point or the Client view, this section displays the configuration information of the selected W-IAP or the client.

Table 9: *Contents of the Info Section in the Instant Main Window*

Name	Description
Info section in Virtual Controller view	The **Info** section in the Virtual Controller view displays the following information: • **Name**– Displays the Virtual Controller name. • **Country Code**– Displays the Country in which the Virtual Controller is operating. • **Virtual Controller IP address**– Displays the IP address of the Virtual Controller. • **Management**: Indicates if the W-IAP is managed locally or through W-AirWave. • **Master**– Displays the IP address of the Access Point acting as Virtual Controller. • **OpenDNS Status**– Displays the OpenDNS status. If the OpenDNS status indicates **Not Connected**, ensure that the network connection is up and appropriate credentials are configured for **OpenDNS**. • **Uplink type** – Displays the type of uplink configured on the W-IAP, for example, Ethernet or 3G. • **Uplink status** – Indicates the uplink status. • **Blacklisted clients** – Displays the number of blacklisted clients. • **Internal RADIUS Users** – Displays the number of internal RADIUS users. • **Internal Guest Users** – Displays the number of internal guest users. • **Internal User Open Slots**– Displays the available slots for user configuration as supported by the W-IAP model.
Info section in Network view	The **Info** section in the Network view displays the following information: • **Name** – Displays the name of the network. • **Status** – Displays the status of the network. • **Type** – Displays the type of network, for example, Employee, Guest, or Voice. • **IP Assignment**– Indicates if the W-IAP clients are assigned IP address from the network that the Virtual Controller is connected to, or from an internal auto-generated IP scope from the Virtual Controller. • **Access**– Indicates the level of access control configured for the network. • **WMM DSCP**–Displays WMM DSCP mapping details. • **Security level**– Indicates the type of user authentication and data encryption configured for the network. The **info** section for WLAN SSIDs also indicates status of Captive Portal and CALEA ACLs and provides a link to upload certificates for internal server. For more information, see Uploading Certificates on page 173.

Info section in Access Point view	The **Info** section in the Access Point view displays the following information:
	• **Name** – Displays the name of the selected W-IAP.
	• **IP Address** – Displays the IP address of the W-IAP.
	• **Mode** – Displays the mode in which the AP is configured to operate:
	  ◦ In **Access** mode, the W-IAP serves clients, while also monitoring for rogue APs in the background.
	  ◦ In **Monitor** mode, the W-IAP acts as a dedicated monitor, scanning all channels for rogue APs and clients.
	• **Spectrum** – Displays the status of the spectrum monitor.
	• **Clients** – Number of clients associated with the W-IAP.
	• **Type** – Displays the model number of the W-IAP.
	• **Zone** – Displays AP zone details.
	• **CPU Utilization** – Displays the CPU utilization in percentage.
	• **Memory Free** – Displays the memory availability of the W-IAP in MB.
	• **Serial number** – Displays the serial number of the W-IAP.
	• **MAC**– Displays the MAC address.
	• **From Port**– Displays the port from where the slave W-IAP is learned in hierarchy mode.

Info section in Client view	The **Info** section in the Client view displays the following information: • **Name**– Displays the name of the client.

Table 9: *Contents of the Info Section in the Instant Main Window*

Name	Description
	• **IP Address**– Displays IP address of the client. • **MAC Address**– Displays MAC Address of the client. • **OS**– Displays the Operating System that is running on the client. • **Network**– Indicates the network to which the client is connected. • **Access Point**– Indicates the W-IAP to which the client is connected. • **Channel**– Indicates the channel that is currently used by the client. • **Type**– Displays the channel type on which client is broadcasting. • **Role**–Displays the role assigned to the client.

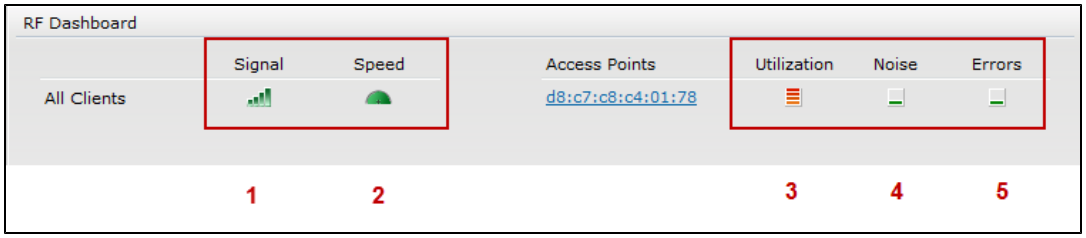
RF Dashboard

The **RF Dashboard** section lists the W-IAPs that exceed the utilization, noise, or error threshold. It also shows the clients with low speed or signal strength in the network and the RF information for the W-IAP to which the client is connected.

The W-IAP names are displayed as links. When a W-IAP is clicked, the W-IAP configuration information is displayed in the Info section and the RF Dashboard section is displayed at the bottom left corner of the Instant main window.

The following figure shows an example of the RF dashboard with Utilization, Band frames, Noise Floor, and Errors details:

Figure 16 *RF Dashboard in the Monitoring Pane*



The following table describes the icons available on the RF Dashboard pane:

Table 10: *RF Dashboard Icons*

Icon	Name	Description
1	Signal Icon	Displays the signal strength of the client. Depending on the signal strength of the client, the color of the lines on the Signal bar changes from Green > Orange > Red. • Green– Signal strength is more than 20 decibels. • Orange– Signal strength is between 15-20 decibels. • Red– Signal strength is less than 15 decibels. To view the signal graph for a client, click on the signal icon next to the client in the **Signal** column.
2	Speed icon	Displays the data transfer speed of the client. Depending on the data transfer speed of the client, the color of the Signal bar changes from Green > Orange > Red. • Green– Data transfer speed is more than 50 percent of the maximum speed supported by the client. • Orange– Data transfer speed is between 25-50 percent of the maximum speed supported by the client. • Red– Data transfer speed is less than 25 percent of the maximum speed supported by the client. To view the data transfer speed graph of a client, click on the speed icon against the client in the **Speed** column.
3	Utilization icon	Displays the radio utilization rate of the W-IAPs. Depending on the percentage of utilization, the color of the lines on the Utilization icon changes from Green > Orange > Red. • Green– Utilization is less than 50 percent. • Orange– Utilization is between 50-75 percent. • Red– Utilization is more than 75 percent. To view the utilization graph of a W-IAP, click the Utilization icon next to the W-IAP in the Utilization column.
4	Noise icon	Displays the noise floor details for the W-IAPs. Noise is measured in decibels/meter. Depending on the noise floor, the color of the lines on the Noise icon changes from Green > Orange > Red. • Green– Noise floor is more than 87 dBm. • Orange– Noise floor is between 80 dBm-87 dBm. • Red– Noise floor is less than 80 dBm. To view the noise floor graph of a W-IAP, click the noise icon next to the W-IAP in the Noise column.
5	Errors icon	Displays the errors for the W-IAPs. Depending on the errors, color of the lines on the Errors icon changes from Green > Yellow > Red. • Green– Errors are less than 5000 frames per second. • Orange– Errors are between 5000-10000 frames per second. • Red– Errors are more than 10000 frames per second. To view the errors graph of a W-IAP, click the **Errors** icon next to the W-IAP in the **Errors** column.

RF Trends

The **RF Trends** section displays the following graphs for the selected AP and the client. To view the details on the graphs, click the graphs and hover the mouse on a data point:

Figure 17 *RF Trends for Access Point*

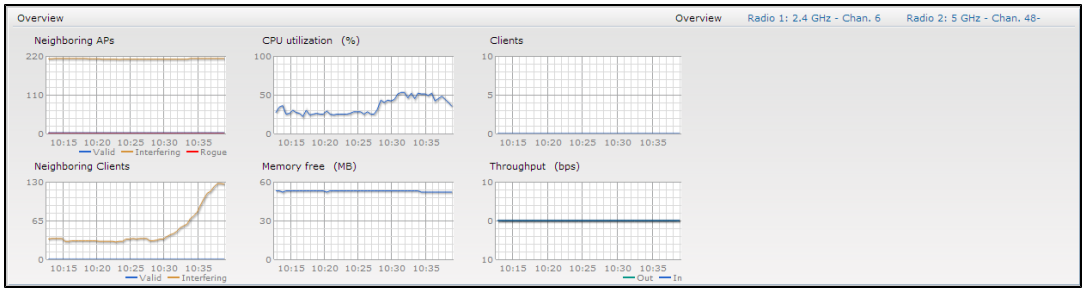
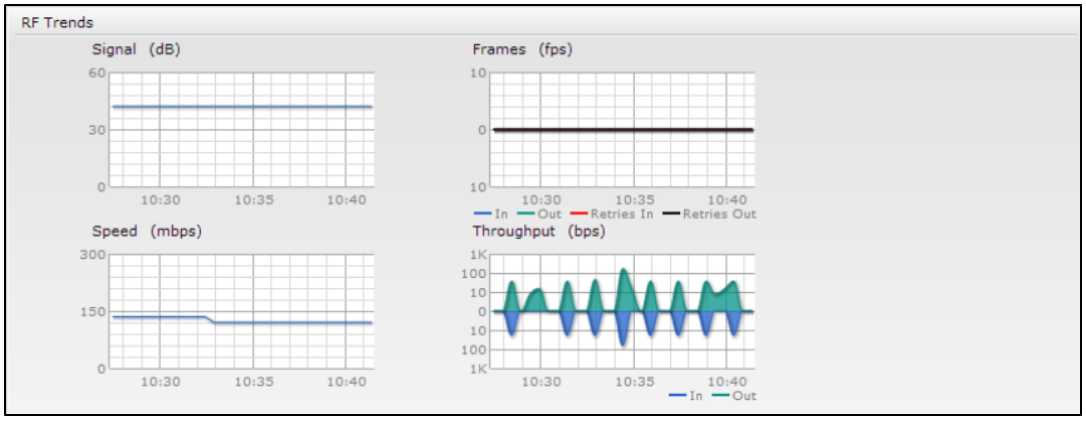


Figure 18 *RF Trends for Clients*

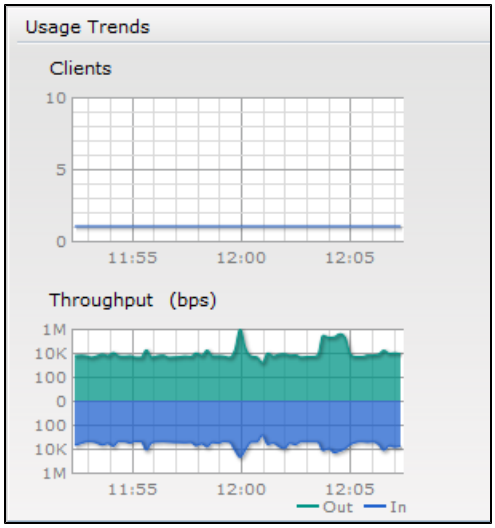


Usage Trends

The **Usage Trends** displays the following graphs:

- Clients – In the default view, the Clients graph displays the number of clients that were associated with the Virtual Controller in the last 15 minutes. In Network or Access Points view, this graph displays the number of clients that were associated with the selected network or W-IAP in the last 15 minutes.
- Throughput– In the default view, the Throughput graph displays the incoming and outgoing throughput traffic for the Virtual Controller in the last 15 minutes. In the Network or Access Points view, this graph displays the incoming and outgoing throughput traffic for the selected network or W-IAP in the last 15 minutes.

Figure 19 *Usage Trends Graphs in the Default View*



The following table describes the graphs displayed in the Network view:

Table 11: *Network View – Graphs and Monitoring Procedures*

Graph Name	Description	Monitoring Procedure
Clients	The Clients graph shows the number of clients associated with the network for the last 15 minutes. To see an enlarged view, click the graph. • The enlarged view provides Last, Minimum, Maximum, and Average statistics for the number of clients associated with the Virtual Controller for the last 15 minutes. • To see the exact number of clients in the Instant network at a particular time, move the cursor over the graph line.	To check the number of clients associated with the network for the last 15 minutes, 1. Log in to the Instant UI. The Virtual Controller view appears. This is the default view. 2. In the **Networks** tab, click the network for which you want to check the client association. The Network view is displayed. 3. Study the Clients graph in the **Usage Trends** pane. For example, the graph shows that one client is associated with the selected network at 12:00 hours.
Throughput	The Throughput graph shows the throughput of the selected network for the last 15 minutes. • Outgoing traffic – Throughput for outgoing traffic is displayed in green. Outgoing traffic is shown above the median line. • Incoming traffic – Throughput for incoming traffic is displayed in blue. Incoming traffic is shown below the median line. To see an enlarged view, click the graph. • The enlarged view provides Last, Minimum, Maximum, and Average statistics for the incoming and outgoing traffic throughput of the network for the last 15 minutes. To see the exact throughput of the selected network at a particular time, move the cursor over the graph line.	To check the throughput of the selected network for the last 15 minutes, 1. Log in to the Instant UI. The Virtual Controller view is displayed. This is the default view. 2. In the **Networks** tab, click the network for which you want to check the client association. The Network view is displayed. 3. Study the Throughput graph in the **Usage Trends** pane. For example, the graph shows 22.0 Kbps incoming traffic throughput for the selected network at 12:03 hours.

The following table describes the graphs displayed in the Access Point view:

Table 12: *Access Point View – Usage Trends and Monitoring Procedures*

Graph Name	Description	Monitoring Procedure
Neighboring APs	The Neighboring APs graph shows the number of APs heard by the selected W-IAP: • Valid APs: An AP that is part of the enterprise providing WLAN service. • Interfering APs: An AP that is seen in the RF environment but is not connected to the network. • Rogue APs: An unauthorized AP that is plugged into the wired side of the network. To see the number of different types of neighboring APs for the last 15 minutes, move the cursor over the respective graph lines.	To check the neighboring APs detected by the W-IAP for the last 15 minutes, 1. Log in to the Instant UI. The Virtual Controller view is displayed. This is the default view. 2. In the **Access Points** tab, click the W-IAP for which you want to monitor the client association. The W-IAP view is displayed. 3. Study the Neighboring APs graph in the **Overview** section. For example, the graph shows that 148 interfering APs are detected by the W-IAP at 12:04 hours.
CPU Utilization	The CPU Utilization graph displays the utilization of CPU for the selected W-IAP. To see the CPU utilization of the W-IAP, move the cursor over the graph line.	To check the CPU utilization of the W-IAP for the last 15 minutes, 1. Log in to the Instant UI. The Virtual Controller view is displayed. This is the default view. 2. In the **Access Points** tab, click the W-IAP for which you want to monitor the client association. The W-IAP view is displayed. 3. Study the CPU Utilization graph in the **Overview** pane. For example, the graph shows that the CPU utilization of the W-IAP is 30% at 12:09 hours.
Neighboring Clients	The Neighboring Clients graph shows the number of clients not connected to the selected AP, but heard by it. • Any client that successfully authenticates with a valid AP and passes encrypted traffic is classified as a valid client. • Interfering: A client associated to any AP and is not valid is classified as an interfering client. To see the number of different types of neighboring clients for the last 15 minutes, move the cursor over the respective graph lines.	To check the neighboring clients detected by the W-IAP for the last 15 minutes, 1. Log in to the Instant UI. The Virtual Controller view is displayed. This is the default view. 2. In the **Access Points** tab, click the W-IAP for which you want to monitor the client association. The W-IAP view is displayed. 3. Study the Neighboring Clients graph in the **Overview** pane. For example, the graph shows that 20 interfering clients were detected by the W-IAP at 12:15 hours.

Table 12: *Access Point View – Usage Trends and Monitoring Procedures*

Graph Name	Description	Monitoring Procedure
Memory free (MB)	The memory free graph displays the memory availability of the W-IAP in MB. To see the free memory of the W-IAP, move the cursor over the graph line.	To check the free memory of the W-IAP for the last 15 minutes, 1. Log in to the Instant UI. The Virtual Controller view is displayed. This is the default view. 2. In the **Access Points** tab, click the W-IAP for which you want to monitor the client association. The W-IAP view is displayed. 3. Study the Memory free graph in the **Overview** pane. For example, the graph shows that the free memory of the W-IAP is 64 MB at 12:13 hours.
Clients	The Clients graph shows the number of clients associated with the selected W-IAP for the last 15 minutes. To see an enlarged view, click the graph. The enlarged view provides Last, Minimum, Maximum, and Average statistics for the number of clients associated with the W-IAP for the last 15 minutes. To see the exact number of clients associated with the selected W-IAP at a particular time, move the cursor over the graph line.	To check the number of clients associated with the W-IAP for the last 15 minutes, 1. Log in to the Instant UI. The Virtual Controller view is displayed. This is the default view. 2. In the **Access Points** tab, click the W-IAP for which you want to monitor the client association. The W-IAP view is displayed. 3. Study the Clients graph. For example, the graph shows that six clients are associated with the W-IAP at 12:11 hours.
Throughput	The Throughput graph shows the throughput for the selected W-IAP for the last 15 minutes. • Outgoing traffic – Throughput for outgoing traffic is displayed in green. Outgoing traffic is shown about the median line. • Incoming traffic – Throughput for incoming traffic is displayed in blue. Incoming traffic is shown below the median line. To see an enlarged view, click the graph. • The enlarged view provides Last, Minimum, Maximum, and Average statistics for the incoming and outgoing traffic throughput of the W-IAP for the last 15 minutes. To see the exact throughput of the selected W-IAP at a particular time, move the cursor over the graph line.	To check the throughput of the selected W-IAP for the last 15 minutes, 1. Log in to the Instant UI. The Virtual Controller view is displayed. This is the default view. 2. In the **Access Points** tab, click the W-IAP for which you want to monitor the throughput. The W-IAP view is displayed. 3. Study the Throughput graph. For example, the graph shows 44.03 Kbps incoming traffic throughput at 12:08 hours.

The following table describes the RF trends graphs available in the client view:

Table 13: *Client View – RF Trends Graphs and Monitoring Procedures*

Graph Name	Description	Monitoring Procedure
Signal	The Signal graph shows the signal strength of the client for the last 15 minutes. It is measured in decibels. To see an enlarged view, click the graph. The enlarged view provides Last, Minimum, Maximum, and Average signal statistics of the client for the last 15 minutes. To see the exact signal strength at a particular time, move the cursor over the graph line.	To monitor the signal strength of the selected client for the last 15 minutes, 1. Log in to the Instant UI. The Virtual Controller view is displayed. This is the default view. 2. In the **Clients** tab, click the IP address of the client for which you want to monitor the signal strength. The client view is displayed. 3. Study the Signal graph in the RF Trends pane. For example, the graph shows that signal strength for the client is 54.0 dB at 12:23 hours.
Frames	The Frames Graph shows the In and Out frame rate per second of the client for the last 15 minutes. It also shows data for the Retry In and Retry Out frames. • Outgoing frames – Outgoing frame traffic is displayed in green. It is shown above the median line. • Incoming frames – Incoming frame traffic is displayed in blue. It is shown below the median line. • Retry Out – Retries for the outgoing frames are displayed above the median line in black . • Retry In – Retries for the incoming frames are displayed below the median line in red. To see an enlarged view, click the graph. The enlarged view provides Last, Minimum, Maximum, and Average statistics for the In, Out, Retries In, and Retries Out frames. To see the exact frames at a particular time move the cursor over the graph line.	To monitor the In and Out frame rate per second and retry frames for the In and Out traffic, for the last 15 minutes, 1. Log in to the Instant UI. The Virtual Controller view is displayed. This is the default view. 2. In the **Clients** tab, click the IP address of the client for which you want to monitor the frames. The client view is displayed. 3. Study the Frames graph in the RF Trends pane. For example, the graph shows 4.0 frames per second for the client at 12:27 hours.
Speed	The Speed graph shows the data transfer speed for the client. Data transfer is measured in Mbps. To see an enlarged view, click the graph. The enlarged view shows Last, Minimum, Maximum, and Average statistics of the client for the last 15 minutes. To see the exact speed at a particular time, move the cursor over the graph line.	To monitor the speed for the client for the last 15 minutes, 1. Log in to the Instant UI. The Virtual Controller view is displayed. This is the default view. 2. In the **Clients** tab, click the IP address of the client for which you want to monitor the speed. The client view is displayed. 3. Study the Speed graph in the RF Trends pane. For example, the graph shows that the data transfer speed at 12:26 hours is 240 Mbps.
Throughput	The Throughput Graph shows the throughput of the selected client for the last 15 minutes. • Outgoing traffic – Throughput for outgoing traffic is displayed in green. Outgoing traffic is shown above the median line. • Incoming traffic – Throughput for	To monitor the errors for the client for the last 15 minutes, 1. Log in to the Instant UI. The Virtual Controller view is displayed. This is the default view. 2. In the **Clients** tab, click the IP address of the client for which you want to monitor the throughput. The client view is displayed. 3. Study the Throughput graph in the RF Trends pane.

Table 13: *Client View – RF Trends Graphs and Monitoring Procedures*

Graph Name	Description	Monitoring Procedure
	incoming traffic is displayed in blue. Incoming traffic is shown below the median line. To see an enlarged view, click the graph. The enlarged view shows Last, Minimum, Maximum, and Average statistics for the incoming and outgoing traffic throughput of the client for the last 15 minutes. To see the exact throughput at a particular time, move the cursor over the graph line.	For example, the graph shows 1.0 Kbps outgoing traffic throughput for the client at 12:30 hours.

Mobility Trail

The **Mobility Trail** section displays the following mobility trail information for the selected client:

- **Association Time**– The time at which the selected client was associated with a particular W-IAP. The Instant UI shows the client and W-IAP association over the last 15 minutes.
- **Access Point**– The W-IAP name with which the client was associated.

Mobility information about the client is reset each time it roams from one W-IAP to another.

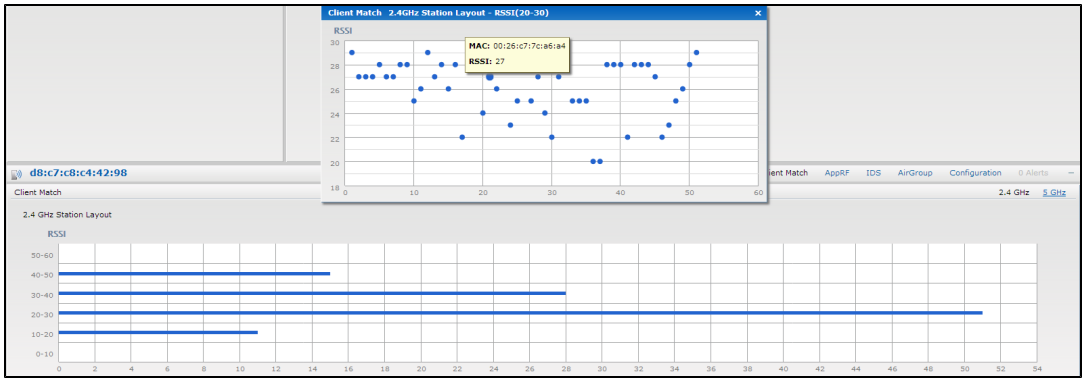
Client Match

If client match is enabled, the **Client Match** link provides a graphical representation of radio map view of an AP and the client distribution on an AP radio.

On clicking an access point in the **Access Points** tab and the **Client Match** link, a stations map view is displayed and a graph is drawn with real-time data points for the AP radio. If the AP supports dual band, you can toggle between 2.4GHz and 5 GHz links in the client match graph area to view the data. When you hover the mouse on the graph, details such as RSSI, client match status, and the client distribution on channels are displayed.

The following figure shows the client distribution details for an AP radio.

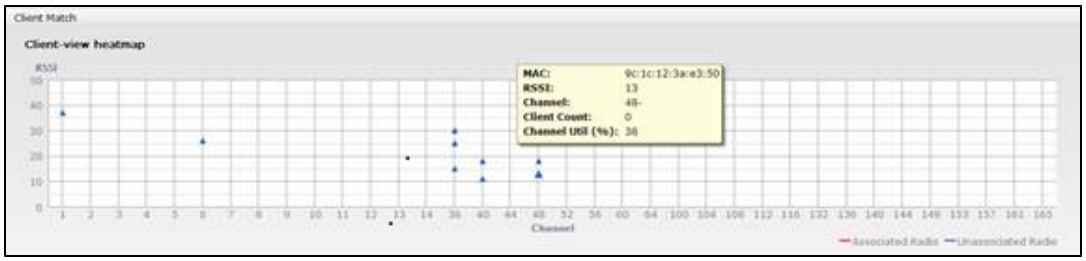
Figure 20 *Client Distribution on AP Radio*



On clicking a client in the **Clients** tab and the **Client Match** link, a graph is drawn with real-time data points for an AP radio map. When you hover the mouse on the graph, details such as RSSI, channel utilization details, and client count on each channel are displayed.

The following figure shows the client view heatmap for an AP radio:

Figure 21 *Channel Availability Map for Clients*



AppRF

The **AppRF** link displays the application traffic summary for W-IAPs and client devices. The **AppRF** link in the activity panel is displayed only if **AppRF visibility** is enabled in the **System** window. For more information on application visibility and AppRF charts, see Application Visibility on page 242.

Spectrum

The spectrum link (in the Access Point view) displays the spectrum data that is collected by a hybrid AP or by a W-IAP that has enabled spectrum monitor. The spectrum data is not reported to the Virtual Controller.

The spectrum link displays the following:

- **Device list** - The device list display consists of a device summary table and channel information for active non Wi-Fi devices currently seen by a spectrum monitor or hybrid AP radio.
- **Channel Utilization and Monitoring** - This chart provides an overview of channel quality across the spectrum. It shows channel utilization information such as channel quality, availability, and utilization metrics as seen by a spectrum monitor for the 2.4 GHz and 5 GHz radio bands. The first bar for each channel represents the percentage of air time used by non Wi-Fi interference and Wi-Fi devices. The second bar indicates the channel quality. A higher percentage value indicates better quality.
- **Channel Details** - When you move your mouse over a channel, the channel details or the summary of the 5 GHz and 2.4 GHz channels as detected by a spectrum monitor are displayed. You can view the aggregate data for each channel seen by the spectrum monitor radio, including the maximum AP power, interference and the Signal-to-Noise and Interference Ratio (SNIR). Spectrum monitors display spectrum analysis data seen on all channels in the selected band, and hybrid W-IAPs display data from the one channel they are monitoring.

For more information on spectrum monitoring, see Spectrum Monitor on page 309.

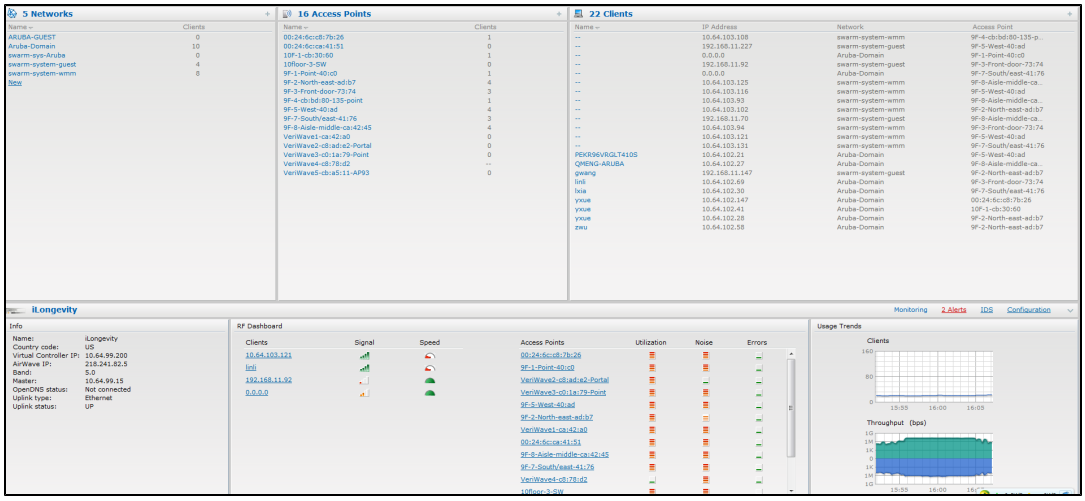
Alerts

Alerts are generated when a user encounters problems while accessing or connecting to a network. The alerts that are generated can be categorized as follows:

- 802.11 related association and authentication failure alerts
- 802.1X related mode and key mismatch, server, and client time-out failure alerts
- IP address related failures - Static IP address or DHCP related alerts.

The following figure shows the contents of details displayed on clicking the **Alerts** link:

Figure 22 *Alerts Link*



The **Alerts** link displays the following types of alerts:

- Client Alerts
- Active Faults
- Fault History

Table 14: *Types of Alerts*

Type of Alert	Description	Information Displayed
Client Alerts	The **Client alerts** occur when clients are connected to the Instant network.	A client alert displays the following fields: • **Timestamp**– Displays the time at which the client alert was recorded. • **MAC address**– Displays the MAC address of the client that caused the alert. • **Description**– Provides a short description of the alert. • **Access Points**– Displays the IP address of the W-IAP to which the client is connected. • **Details**– Provides complete details of the alert.
Active Faults	The **Active Faults** occur in the event of a system fault.	An **Active Faults** consists of the following fields: • **Time**– Displays the system time when an event occurs. • **Number**– Indicates the number of sequence. • **Description**– Displays the event details.
Fault History	The **Fault History** alerts occur in the event of a system fault.	The **Fault History** displays the following information: • **Time**– Displays the system time when an event occurs. • **Number**– Indicates the number of sequence. • **Cleared by**– Displays the module which cleared this fault. • **Description**– Displays the event details.

The following figures show the client alerts, fault history, and active faults:

Figure 23 *Client Alerts*

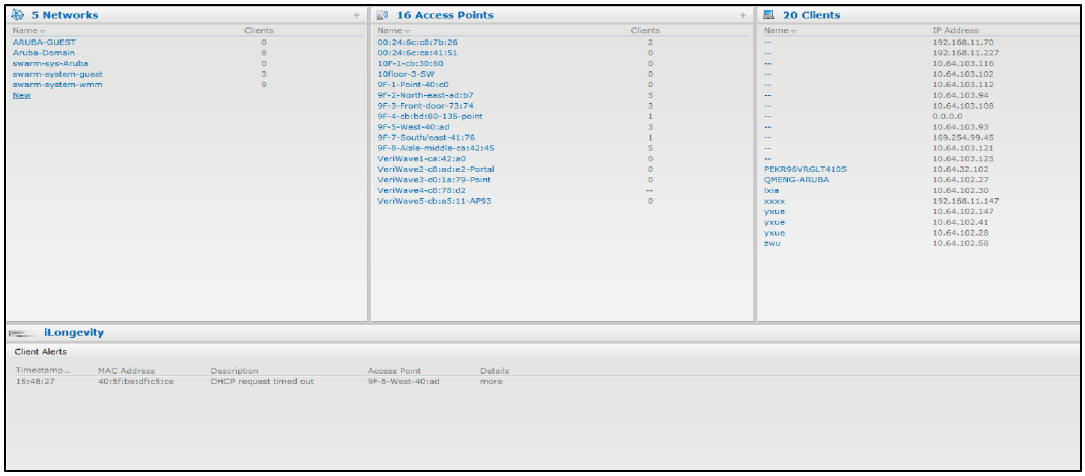


Figure 24 *Fault History*

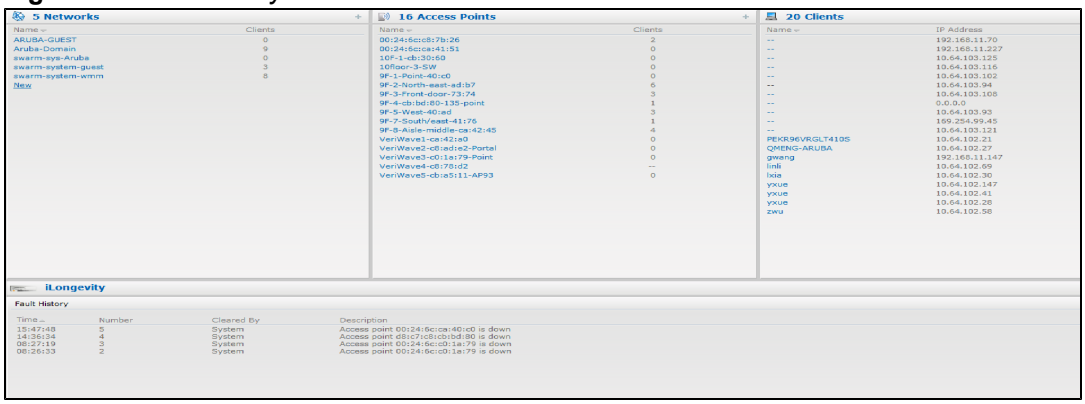
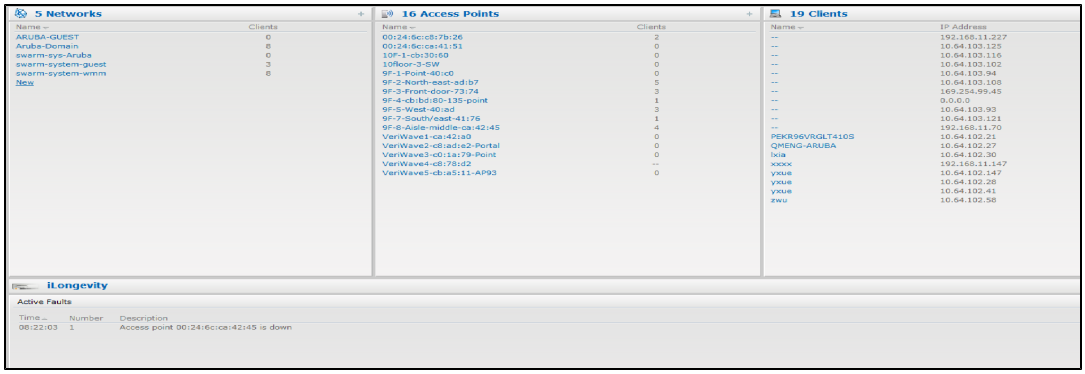


Figure 25 *Active Faults*



The following table displays a list of alerts that are generated in the W-IAP network:

Table 15: *Alerts list*

Type Code	Description	Details	Corrective Actions
100101	Internal error	The W-IAP has encountered an internal error for this client.	Contact the Dell customer support team.
100102	Unknown SSID in association request	The W-IAP cannot allow this client to associate, because the association request received contains an unknown SSID.	Identify the client and check its Wi-Fi driver and manager software.
100103	Mismatched authentication/encryption setting	The W-IAP cannot allow this client to associate, because its authentication or encryption settings do not match W-IAP's configuration.	Ascertain the correct authentication or encryption settings and try to associate again.
100104	Unsupported 802.11 rate	The W-IAP cannot allow this client to associate because it does not support the 802.11 rate requested by this client.	Check the configuration on the W-IAP to see if the desired rate can be supported; if not, consider replacing the W-IAP with another model that can support the rate.
100105	Maximum capacity reached on W-IAP	The W-IAP has reached maximum capacity and cannot accommodate any more clients.	Consider expanding capacity by installing additional W-IAPs or balance load by relocating W-IAPs.
100206	Invalid MAC Address	The W-IAP cannot authenticate this client because the client's MAC address is not valid.	This condition may be indicative of a misbehaving client. Try to locate the client device and check its hardware and software.
100307	Client blocked due to repeated authentication failures	The W-IAP is temporarily blocking the 802.1X authentication request from this client, because the credentials provided are rejected by the RADIUS server too many times.	Identify the client and check its 802.1X credentials.
100308	RADIUS server connection failure	The W-IAP cannot authenticate this client using 802.1X, because the RADIUS server did not respond to the authentication request.	If the W-IAP is using the internal RADIUS server, it is recommended that you check the related configuration as well as the installed certificate and passphrase. If the W-IAP is using an external RADIUS server, check if there are any issues with the RADIUS server and try connecting again.

Table 15: *Alerts list*

Type Code	Description	Details	Corrective Actions
100309	RADIUS server authentication failure	The W-IAP cannot authenticate this client using 802.1X , because the RADIUS server rejected the authentication credentials (password and so on) provided by the client.	Ascertain the correct authentication credentials and log in again.
100410	Integrity check failure in encrypted message	The W-IAP cannot receive data from this client , because the integrity check of the received message (MIC) has failed.	Check the encryption setting on the client and on the W-IAP.
100511	DHCP request timed out	This client did not receive a response to its DHCP request in time.	Check the status of the DHCP server in the network.

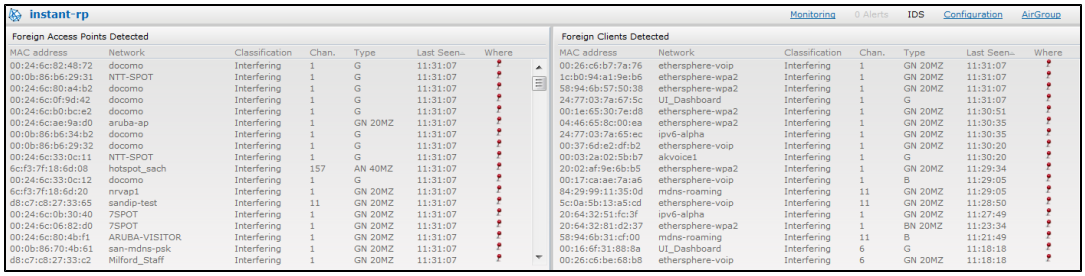
IDS

The **IDS** link displays a list of foreign APs and foreign clients that are detected in the network. It consists of the following sections:

- Foreign Access Points Detected– Lists the APs that are not controlled by the Virtual Controller. The following information is displayed for each foreign AP:
  - MAC address– Displays the MAC address of the foreign AP.
  - Network– Displays the name of the network to which the foreign AP is connected.
  - Classification– Displays the classification of the foreign AP, for example, Interfering W-IAP or Rogue W-IAP.
  - Channel– Displays the channel in which the foreign AP is operating.
  - Type– Displays the Wi-Fi type of the foreign AP.
  - Last seen– Displays the time when the foreign AP was last detected in the network.
  - Where– Provides information about the W-IAP that detected the foreign AP. Click the pushpin icon to view the information.
- Foreign Clients Detected– Lists the clients that are not controlled by the Virtual Controller. The following information is displayed for each foreign client:
  - MAC address– Displays the MAC address of the foreign client.
  - Network– Displays the name of the network to which the foreign client is connected.
  - Classification– Displays the classification of the foreign client: Interfering client.
  - Channel– Displays the channel in which the foreign client is operating.
  - Type– Displays the Wi-Fi type of the foreign client.
  - Last seen– Displays the time when the foreign client was last detected in the network.
  - Where– Provides information about the W-IAP that detected the foreign client. Click the pushpin icon to view the information.

The following figure shows an example for the intrusion detection log.

Figure 26 *Intrusion Detection*



For more information on the intrusion detection feature, see Intrusion Detection on page 296.

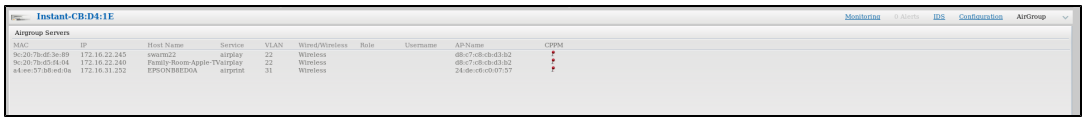
AirGroup

This **AirGroup** link provides an overall view of your AirGroup configuration. Click each field to view or edit the settings.

- **MAC** – Displays the MAC address of the AirGroup servers.
- **IP** – Displays the IP address of the AirGroup servers.
- **Host Name** – Displays the machine name or hostname of the AirGroup servers.
- **Service**– Displays the type of the services such as AirPlay or AirPrint.
- **VLAN**– Displays VLAN details of the AirGroup servers.
- **Wired/Wireless** – Displays if the AirGroup server is connected via wired or wireless interface.
- **Role**–Displays the user role if the server is connected through 802.1X authentication. If the server is connected through PSK or open authentication, this field is blank.
- **Group**–Displays the group.
- **CPPM**– By clicking on this, you get details of the registered rules in ClearPass Policy Manager (CPPM) for this server.
- **MDNS Cache**– By clicking on this, you receive MDNS record details of a particular server.

The following figure shows the AirGroup server details available on clicking the **AirGroup** link:

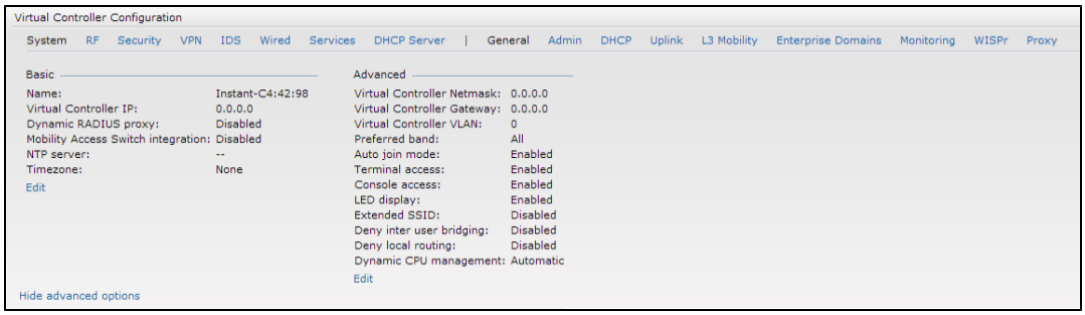
Figure 27 *AirGroup Link*



Configuration

The **Configuration** link provides an overall view of your Virtual Controller, Access Points, and WLAN SSID configuration. The following figure shows the Virtual Controller configuration details displayed on clicking the **Configuration** link.

Figure 28 *Configuration Link*



W-AirWave Setup

W-AirWave is a solution for managing rapidly changing wireless networks. When enabled, W-AirWave allows you to manage the Instant network. For more information on W-AirWave, see Managing a W-IAP from W-AirWave on page 275. The W-AirWave status is displayed at the bottom of the Instant main window. If the W-AirWave status is **Not Set Up**, click the **Set Up Now** link to configure W-AirWave. The **System** window is displayed with **Admin** tab selected.

Pause/Resume

The **Pause/Resume** link is located at the bottom right corner of the Instant main window.

Click the **Pause** link to pause the automatic refreshing of the Instant U after every 15 seconds by default. The Instant UI is automatically refreshed after every 15 seconds by default. When the automatic refreshing is paused, the **Pause** link changes to **Resume**. Click the **Resume** link to resume automatic refreshing.

Automatic refreshing allows you to get the latest information about the network and network elements. You can use the **Pause** link when you want to analyze or monitor the network or a network element, and therefore do not want the user interface to refresh.

Views

Depending on the link or tab that is clicked, the Instant displays information about the Virtual Controller, Wi-Fi networks, W-IAPs, or the clients in the Info section. The views on the Instant main window are classified as follows:

- Virtual Controller view– The Virtual Controller view is the default view. This view allows you to monitor the Instant network. This view allows you to monitor the Instant network.
- The following Instant UI elements are available in this view:
  - Tabs– Networks, Access Points, and Clients. For detailed information about the tabs, see Tabs on page 45.
  - Links– Monitoring, Client Alerts, and IDS. The Spectrum link is visible if you have configured the W-IAP as a spectrum monitor. These links allow you to monitor the Instant network. For more information about these links, see Monitoring on page 57, IDS on page 71, Alerts on page 67, and Spectrum Monitor on page 309.
- Network view– The Network view provides information that is necessary to monitor a selected wireless network. All Wi-Fi networks in the Instant network are listed in the **Networks** tab. Click the name of the network that you want to monitor. Network view for the selected network is displayed.
- Instant Access Point view– The Instant Access Point view provides information that is necessary to monitor a selected W-IAP. All W-IAPs in the Instant network are listed in the **Access Points** tab. Click the name of the W-IAP that you want to monitor. Access Point view for that W-IAP is displayed.
- Client view– The Client view provides information that is necessary to monitor a selected client. In the Client view, all the clients in the Instant network are listed in the **Clients** tab. Click the IP address of the client that you want to monitor. Client view for that client is displayed.

For more information on the graphs and the views, see Monitoring on page 57.

This chapter describes the general configuration tasks to perform when a W-IAP is set up.

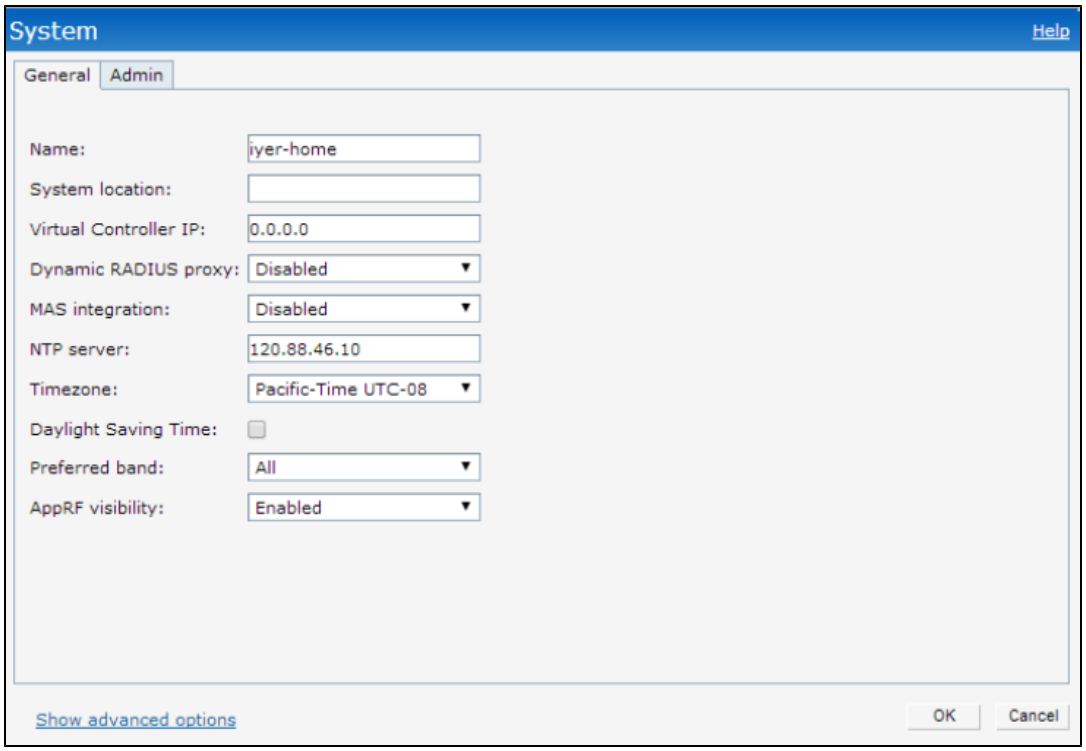
- Basic Configuration Tasks on page 74
- Additional Configuration Tasks on page 78

Basic Configuration Tasks

This section describes the following basic configuration tasks that can be performed in the **System**>**General** tab after a W-IAP is set up:

- Modifying the W-IAP Name on page 74
- Updating Location Details of a W-IAP on page 75
- Configuring Virtual Controller IP Address on page 76
- Configuring Timezone on page 76
- Configuring a Preferred Band on page 75
- Configuring an NTP Server on page 76
- Enabling AppRF Visibility on page 77

The following figure shows an example for the basic configuration settings under the **System**>**General** tab:



For information on Dynamic RADIUS proxy configuration, see Configuring Authentication Servers on page 157.

Modifying the W-IAP Name

You can change the name of a W-IAP by using the Instant UI or CLI.

In the Instant UI

1. Navigate to **System**>**General**.
2. Specify the name of W-IAP in the **Name** text box.
3. Click **OK**.

In the CLI

To change the name:

```
(Instant AP)# name <name>
```

Updating Location Details of a W-IAP

You can update the physical location details of a W-IAP by using the Instant UI or CLI. The system location details are used for retrieving information through the SNMP *sysLocation* MIB object.

In the Instant UI

To update location details:

1. Navigate to **System**>**General**.
2. Specify the location of a W-IAP in the **System location** text box.
3. Click **OK**.

In the CLI

To update location details of a W-IAP:

```
(Instant AP)(config)# syslocation <location-name>
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Configuring a Preferred Band

You can configure a preferred band for a W-IAP by using the Instant UI or the CLI.

In the Instant UI

1. Navigate to **System**>**General**.
2. Select **2.4 GHz**, **5 GHz** or **All** from the **Preferred band** drop-down list for single-radio access points.
3. Click **OK**.

Reboot the W-IAP after configuring the radio profile for the changes to affect.

In the CLI

To configure a preferred band:

```
(Instant AP)(config)# rf-band <band>
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Configuring Virtual Controller IP Address

You can specify a single static IP address that can be used to manage a multi-AP Instant network. This IP address is automatically provisioned on a shadow interface on the W-IAP that takes the role of a Virtual Controller. When a W-IAP becomes a Virtual Controller, it sends three Address Resolution Protocol (ARP) messages with the static IP address and its MAC address to update the network ARP cache.

You can configure the Virtual Controller name and IP address using the Instant UI or CLI.

In the Instant UI

1. Navigate to **System**>**General**.
2. Enter the IP address in **Virtual Controller IP**.
3. Click **OK**.

In the CLI

To configure the Virtual Controller Name and IP address:

```
(Instant AP)(config)# virtual-controller-ip <IP-address>
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Configuring Timezone

You can configure time zone in which the W-IAP must operate by using the Instant or the CLI.

In the Instant UI

To configure time zone:

1. Navigate to **System**>**General**.
2. Select a time zone from the **Timezone** drop-down list.

You can enable daylight saving time (DST) on W-IAPs if the time zone you selected supports the daylight saving time. If the Time Zone selected does not support DST, the **Daylight Saving Time** option is not displayed. When enabled, the Daylight saving time ensures that the W-IAPs reflect the seasonal time changes in the region they serve.

3. To enable daylight saving time, select the **Daylight Saving Time** checkbox.
4. Click **OK**.

In the CLI

To configure time zone:

```
(Instant AP)(config)# clock timezone <name> <hour-offset> <minute-offset>
(Instant AP)(config)# clock summer-time <timezone> recurring <start-week> <start-day> <start-
month> <start-hour> <end-week> <end-day> <end-month> <end-hour>
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Configuring an NTP Server

To facilitate communication between various elements in a network, time synchronization between the elements and across the network is critical. Time synchronization allows you to:

- Trace and track security gaps, network usage, and troubleshoot network issues.
- Validate certificates
- Map an event on one network element to a corresponding event on another.

- Maintain accurate time for billing services and similar.

The Network Time Protocol (NTP) helps obtain the precise time from a server and regulate the local time in each network element. Connectivity to a valid NTP server is required to synchronize the W-IAP clock to set the correct time. If NTP server is not configured in the W-IAP network, a W-IAP reboot may lead to variation in time data.

By default, the W-IAP tries to connect to **pool.ntp.org** to synchronize time. A different NTP server can be configured either from the UI. It can also be provisioned through the DHCP option 42. If the NTP server is configured, it takes precedence over the DHCP option 42 provisioned value. The NTP server provisioned through the DHCP option 42 is used if no server is configured. The default server **pool.ntp.org** is used if no NTP server is configured or provisioned through DHCP option 42.

Reboot the AP to apply the NTP server configuration.

You can configure an NTP server by using the Instant UI or the CLI.

In the Instant UI

To configure an NTP server:

1. Navigate to **System**>**General**.
2. Enter the IP address or the URL (domain name) of the NTP server in the **NTP Server** text box.
3. Click **OK**.
4. Reboot the W-IAP.

In the CLI

To configure an NTP server:

```
(Instant AP)(config)# ntp-server <name>
(Instant AP)(config)# end
(Instant AP)# commit apply
```

To check the NTP status and association, run the **show clock** and **show process** commands.

Enabling AppRF Visibility

If your W-IAP supports the AppRF feature, you can enable AppRF visibility to view the AppRF statistics for a W-IAP or the clients associated with a W-IAP. For more information on the procedure for enabling AppRF visualization, see Enabling Application Visibility on page 241.

Changing Password

You can update your password details by using the Instant UI or the CLI.

In the Instant UI

1. Navigate to **System**>**Admin**.
2. Under **Local**, provide a new password that you would like the admin users to use.
3. Click **OK**.

In the CLI

To change password for the admin user:

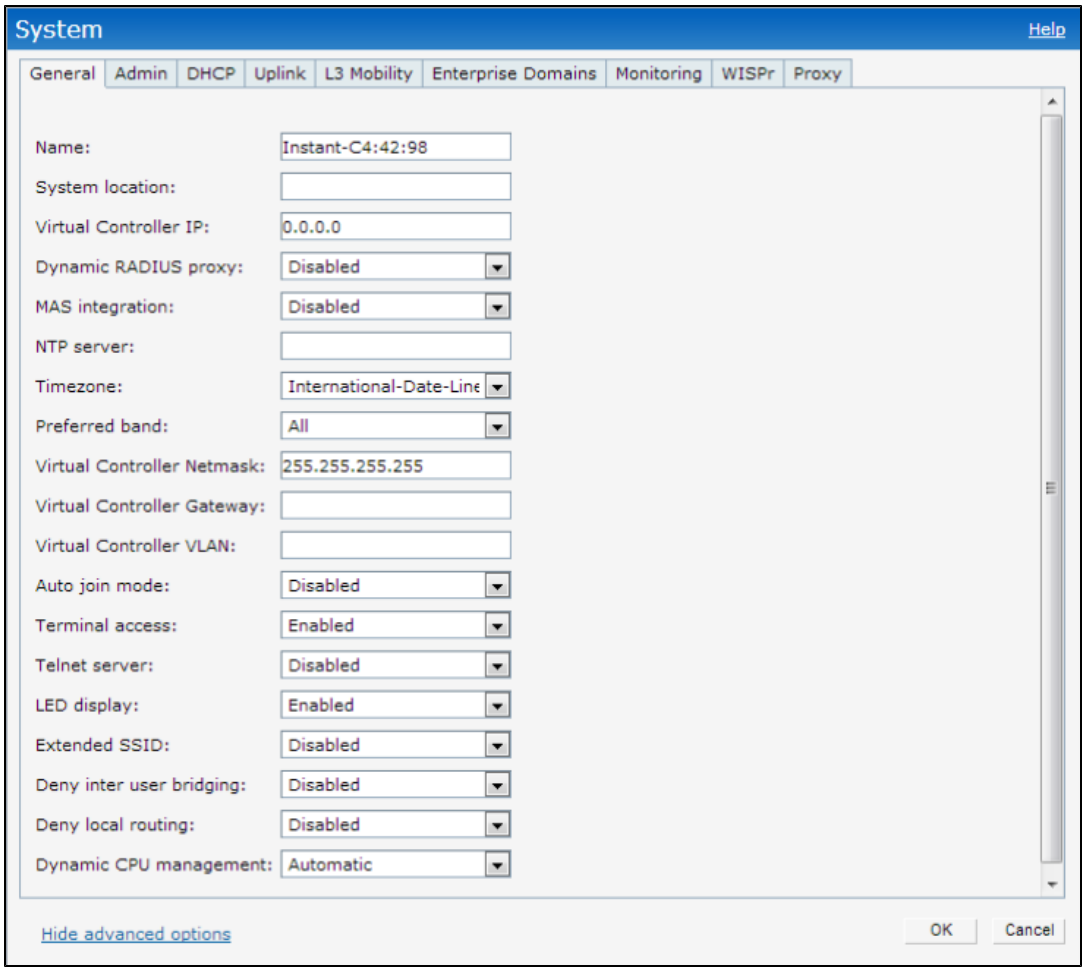
```
(Instant AP)(config)# mgmt-user <username> [password]
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Additional Configuration Tasks

This section describes the following additional tasks that can be performed after a W-IAP is set up:

- Configuring Virtual Controller VLAN on page 78
- Configuring Auto Join Mode on page 79
- Configuring Terminal Access on page 80
- Configuring Console Access on page 80
- Configuring LED Display on page 81
- Configuring Additional WLAN SSIDs on page 81
- Preventing Inter-user Bridging on page 82
- Preventing Local Routing between Clients on page 82
- Enabling Dynamic CPU Management on page 83

The following figure shows the additional configuration options available under the **System**>**General** tab:



Configuring Virtual Controller VLAN

NOTE

The IP configured for the Virtual Controller can be in the same subnet as W-IAP or can be in a different subnet. Ensure that you configure the Virtual Controller VLAN, gateway, and subnet mask details only if the Virtual Controller IP is in a different subnet.

You can configure the Virtual Controller VLAN by using Instant UI or CLI.

In the Instant UI

1. Navigate to **System**>**General**> **Show advanced options**. The advanced options are displayed.
2. Enter subnet mask details in **Virtual Controller Netmask**.
3. Enter a gateway address in **Virtual Controller Gateway**.
4. Enter Virtual Controller VLAN in **Virtual Controller VLAN**.

Ensure that Virtual Controller VLAN is not the same as native VLAN of the W-IAP.

5. Click **OK**.

In the CLI

To configure the Virtual Controller Name and IP address:

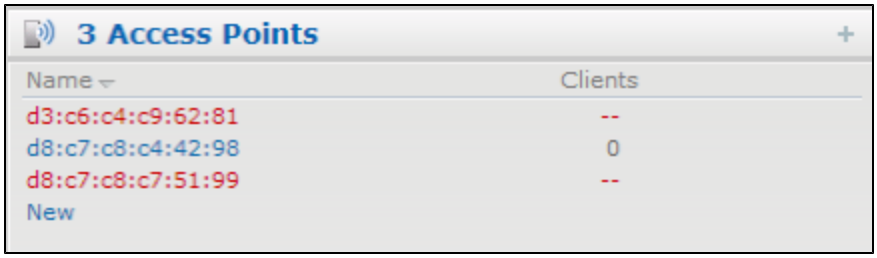
```
(Instant AP)(config)# virtual-controller-vlan <vcvlan> <vcmask> <vcgw>
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Configuring Auto Join Mode

The auto join mode feature allows W-IAPs to automatically discover the Virtual Controller and join the network.

The **Auto Join Mode** feature is enabled by default. If the auto join mode feature is disabled, a **New** link is displayed in the **Access Points** tab. Click this link to add W-IAPs to the network. If this feature is disabled, the inactive W-IAPs are displayed in red as shown in the following figure:

Figure 29 *Inactive W-IAPs*



Enabling or Disabling Auto Join Mode

You can enable or disable auto join mode by using the Instant UI or CLI.

In the Instant UI

To enable or disable auto join mode:

1. Navigate to **System**>**General**>**Show advanced options**.
2. Select **Disabled** or **Enabled** from the **Auto join mode** drop-down list to deny or allow APs to join the network.
3. Click **OK**.

In the CLI

To disable auto join mode:

```
(Instant AP)(config)# no allow-new-aps
(Instant AP)(config)# end
(Instant AP)# commit apply
```

To enable auto join mode:

```
(Instant AP)(config)# allow-new-aps
```

```
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Configuring Terminal Access

When terminal access is enabled, you can access the Instant CLI through SSH or Telnet server. The terminal access is enabled by default.

You can enable or disable terminal access to a W-IAP by using the Instant UI or CLI.

In the Instant UI

1. Navigate to **System**>**General**>**Show advanced options**.
2. Select **Disabled** or **Enabled** from the **Terminal access** drop-down list.
3. To enable Telnet server based access, select **Enabled** from the **Telnet server** drop-down list.
4. Click **OK**.

In the CLI

To enable terminal access:

```
(Instant AP)(config)# terminal-access
(Instant AP)(config)# end
(Instant AP)# commit apply
```

To enable access to the Instant CLI through Telnet:

```
(Instant AP)(config) # telnet-server
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Configuring Console Access

You can access a W-IAP console through a serial port to configure or debug system errors. You can enable or disable console access to a W-IAP through the Instant UI or CLI.

In the Instant UI

1. Navigate to **System**>**General**>**Show advanced options**.
2. Select **Disabled** or **Enabled** from the **Console access** drop-down list. By default, the console access is enabled. When disabled, the W-IAP console cannot be accessed through the serial port.
3. Click **OK**.

In the CLI

To enable console access:

```
(Instant AP)(config)# console
(Instant AP)(console)# enable
(Instant AP)(console)# end
(Instant AP)# commit apply
```

To disable console access:

```
(Instant AP)(config)# console
(Instant AP)(console)# disable
(Instant AP)(console)# end
(Instant AP)# commit apply
```

To view the console settings:

```
(Instant AP)# show console-settings
```

Configuring LED Display

The LED display is always in the **Enabled** mode during the a W-IAP reboot.

You can enable or disable LED Display for a W-IAP using the Instant UI or CLI.

In the Instant UI

To enable or disable LED display for all W-IAPs in a cluster, perform the following steps:

1. Navigate to **System** > **General** > **Show advanced options**.
2. From the **LED Display** drop-down list, select **Enabled** to enable LED display or **Disabled** to turn off the LED display.
3. Click **OK**.

In the CLI

To enable LED display:

```
(Instant AP)(config)# led-off
(Instant AP)(config)# end
(Instant AP)# commit apply
```

To disable LED display:

```
(Instant AP)(config)# no led-off
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Configuring Additional WLAN SSIDs

The number of SSIDs allowed on each W-IAP depends on the W-IAP platform. The following table describes the number of SSIDs supported on each platform:

W-IAP Platform	No. of SSIDs supported with Extended SSID disabled	No. of SSIDs supported with Extended SSID enabled
IAP-175P/175AC, W-IAP104/105, and W-IAP108/109	6	8
All other W-IAPs (excluding IAP-175P/175AC, W-IAP104/105, and W-IAP108/109)	14	16

Enabling the Extended SSID

Extended SSID is enabled by default in the factory default settings of APs. This disables mesh in the factory default settings.

You can configure additional SSIDs by using the Instant UI or CLI.

In the Instant UI

1. Navigate to **System**>**General**>**Show advanced options** link.
2. In the **General** tab, select **Enabled** from the **Extended SSID** drop-down list.
3. Click **OK**.

4. Reboot the W-IAP to apply the changes. After you enable the option and reboot the W-IAP, the Wi-Fi and mesh links are disabled automatically.

In the CLI

To enable the extended SSIDs:

```
(Instant AP)(config)# extended-ssid
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Preventing Inter-user Bridging

If you have security and traffic management policies defined in upstream devices, you can disable bridging traffic between two clients connected to the same AP on the same VLAN. When inter-user bridging is denied, the clients can connect to the Internet but cannot communicate with each other, and the bridging traffic between the clients is sent to the upstream device to make the forwarding decision.

You can disable inter-user bridging through the Instant UI or CLI.

In the Instant UI

To prevent inter-user bridging:

1. Navigate to **System**>**General**>**Show advanced options**.
2. From the **Deny inter user bridging** drop-down list, select **Enabled** to prevent traffic between two clients connected to a W-IAP on the same VLANs.
3. Click **OK**.

In the CLI

To deny inter-user bridging:

```
(Instant AP)(config)# deny-inter-user-bridging
(Instant AP)(config)# end
(Instant AP)# commit apply
```

To deny inter-user bridging for the WLAN SSID clients:

```
(Instant AP)(config)# wlan ssid-profile <ssid-profile>
(Instant AP) (SSID Profile <ssid-profile>)# deny-inter-user-bridging
(Instant AP) (SSID Profile <ssid-profile>)# end
(Instant AP)# commit apply
```

Preventing Local Routing between Clients

If you have security and traffic management policies defined in upstream devices, you can disable routing traffic between two clients connected to the same W-IAP on different VLANs. When local routing is disabled, the clients can connect to the Internet but cannot communicate with each other, and the routing traffic between the clients is sent to the upstream device to make the forwarding decision.

You can disable local routing through the Instant UI or CLI.

In the Instant UI

To disable local routing:

1. Navigate to **System**>**General**>**Show advanced options**.
2. From the **Deny local routing** drop-down list, select **Enabled** to prevent local routing traffic between two clients connected to a W-IAP on different VLANs.
3. Click **OK**.

In the CLI

To disable local routing:

```
(Instant AP)(config)# deny-local-routing
(Instant AP)(config)# end
(Instant AP)# commit apply
```

To deny local routing for the WLAN SSID clients:

```
(Instant AP)(config)# wlan ssid-profile <ssid-profile>
(Instant AP) (SSID Profile <ssid-profile>)# deny-local-routing
(Instant AP) (SSID Profile <ssid-profile>)# end
(Instant AP)# commit apply
```

Enabling Dynamic CPU Management

W-IAPs perform various functions such as wireless client connectivity and traffic flows, wired client connectivity and traffic flows, wireless security, network management, and location tracking. Like with any network element, a W-IAP can be subject to heavy loads. In such a scenario, it is important to prioritize the platform resources across different functions. Typically, the W-IAPs manage resources automatically in real-time. However, under special circumstances, if dynamic resource management needs to be enforced or disabled altogether, the dynamic CPU management feature settings can be modified.

You can configure the dynamic CPU management feature by using the Instant UI or CLI.

In the Instant UI

To enable or disable the management plane protection:

1. Click **System** > **General**>**Show Advanced Options**.
2. Select any of the following options from the **Dynamic CPU Management** drop-down list.
   - **Automatic** – When selected, the CPU management is enabled or disabled automatically during run-time. This decision is based on real-time load calculations taking into account all different functions that the CPU needs to perform. This is the default and recommended option.
   - **Always disabled on all APs** – When selected, this setting manually disables CPU management on all APs, typically for small networks. This setting protects user experience.
   - **Always enabled on APs** – When selected, the client and network management functions are protected. This setting helps in large networks with high client density.
3. Click **OK**.

In the CLI

```
(Instant AP)(config)# dynamic-cpu-mgmt {auto| enable| disable}
```

This chapter describes the procedures for configuring settings that are specific to a W-IAP in the cluster.

- Modifying the W-IAP Hostname on page 84
- Configuring Zone Settings on a W-IAP on page 84
- Specifying a Method for Obtaining IP Address on page 85
- Configuring External Antenna on page 86
- Configuring Radio Profiles for a W-IAP on page 87
- Configuring Uplink VLAN for a W-IAP on page 88
- Master Election and Virtual Controller on page 89
- Adding a W-IAP to the Network on page 91
- Removing a W-IAP from the Network on page 91

Modifying the W-IAP Hostname

You can change the hostname of a W-IAP through the Instant UI or CLI.

In the Instant UI

1. In the **Access Points** tab, click the W-IAP you want to rename. The **edit** link is displayed.
2. Click the **edit** link. The edit window for modifying W-IAP details is displayed.
3. Edit the W-IAP name in **Name**. You can specify a name of up to 32 ASCII characters.
4. Click **OK**.

In the CLI

To change the name:

```
(Instant AP)# hostname <name>
```

Configuring Zone Settings on a W-IAP

All APs in a cluster use the same SSID configuration including master and slave W-IAPs. However, if you want to assign an SSID to a specific W-IAP, you can configure zone settings for a W-IAP.

The following constraints apply to the AP zone configuration:

- A W-IAP can belong to only one zone and only one zone can be configured on an SSID.
- If an SSID belongs to a zone, all W-IAPs in this zone can broadcast this SSID. If no W-IAP belongs to the zone configured on the SSID, the SSID is not broadcast.
- If an SSID does not belong to any zone, all W-IAPs can broadcast this SSID.

You can add an AP zone by through the UI or CLI.

For the SSID to be assigned to a W-IAP, the same zone details must be configured on the SSID. For more information on SSID configuration, see Configuring WLAN Settings for an SSID Profile on page 93.

In the Instant UI

1. In the **Access Points** tab, click the W-IAP for which you want to set the zone. The **edit** link is displayed.
2. Click the **edit** link. The edit window for modifying W-IAP details is displayed.
3. Specify the AP zone in **Zone**.
4. Click **OK**.

In the CLI

To change the name:

```
(Instant AP)# zone <name>
```

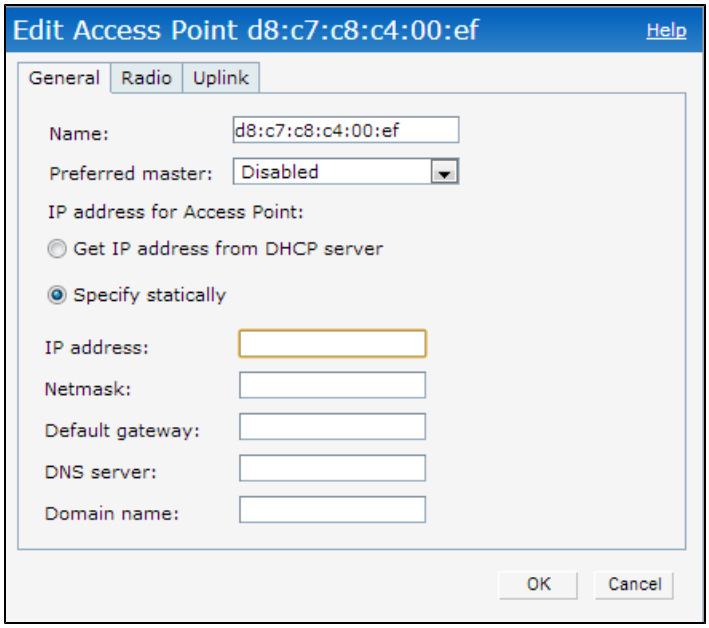
Specifying a Method for Obtaining IP Address

You can either specify a static IP address or allow the W-IAP to obtain an IP address from the DHCP server. By default, the W-IAPs obtain IP address from the DHCP server. You can specify a static IP address for the W-IAP by using the Instant UI or CLI.

In the Instant UI

1. In the **Access Points** tab, click the W-IAP to modify. The **edit** link is displayed.
2. Click the **edit** link. The edit window for modifying the W-IAP details is displayed.

Figure 30 *Configuring W-IAP Settings*



3. Select **Specify statically** option to specify a static IP address. The following fields are displayed:
   a. Enter the new IP address for the W-IAP in the **IP address** text box.
   b. Enter the subnet mask of the network in the **Netmask** text box.
   c. Enter the IP address of the default gateway in the **Default gateway** text box.
   d. Enter the IP address of the DNS server in the **DNS server** text box.
   e. Enter the domain name in the **Domain name** text box.
4. Click **OK** and reboot the W-IAP.

In the CLI

To configure a static IP address:

```
(Instant AP)# ip-address <IP-address> <subnet-mask> <NextHop-IP> <DNS-IP-address> <domain-name>
```

Configuring External Antenna

If your W-IAP has external antenna connectors, you need to configure the transmit power of the system. The configuration must ensure that the system's Equivalent Isotropically Radiated Power (EIRP) is in compliance with the limit specified by the regulatory authority of the country in which the W-IAP is deployed. You can also measure or calculate additional attenuation between the device and antenna before configuring the antenna gain. To know if your AP device supports external antenna connectors, see the *Install Guide* that is shipped along with the AP device.

EIRP and Antenna Gain

The following formula can be used to calculate the EIRP limit related RF power based on selected antennas (antenna gain) and feeder (Coaxial Cable loss):

EIRP = Tx RF Power (dBm)+GA (dB) - FL (dB)

The following table describes this formula:

Table 16: *Formula Variable Definitions*

Formula Element	Description
EIRP	Limit specific for each country of deployment
Tx RF Power	RF power measured at RF connector of the unit
GA	Antenna gain
FL	Feeder loss

Example

For example, the maximum gain that can be configured on a W-IAP134 with AP-ANT-1F dual-band and omni-directional antenna is as follows:

Table 17: *Maximum Antenna Gains*

Frequency Band	Gain (dBi)
2.4-2.5 GHz	2.0dBi
4.9-5.875GHz	5.0dBi

For information on antenna gain recommended by the manufacturer, see dell.com/support.

Configuring Antenna Gain

You can configure antenna gain for APs with external connectors using Instant UI or CLI.

In the Instant UI

1. Navigate to the **Access Point** tab, select the access point to configure and then click **edit**.

2. In the **Edit Access Point** window, select **External Antenna** to configure the antenna gain value. This option is available only for access points that support external antennas, for example, W-IAP134.
3. Enter the antenna gain values in dBm for the 2.4GHz and 5GHz bands.
4. Click **OK**.

In the CLI

To configure external antenna for 5 GHz frequency:

```
(Instant AP)# a-external-antenna <dBi>
```

To configure external antenna for 2,4 GHz frequency:

```
(Instant AP)# g-external-antenna <dBi>
```

Configuring Radio Profiles for a W-IAP

You can configure a radio profile on a W-IAP either manually or by using the Adaptive Radio Management (ARM) feature.

Adaptive Radio Management (ARM) is enabled on Instant by default. It automatically assigns appropriate channel and power settings for the W-IAPs. For more information on ARM, see Adaptive Radio Management on page 232.

Configuring ARM Assigned Radio Profiles for a W-IAP

To enable ARM assigned radio profiles:

1. In the **Access Points** tab, click the W-IAP to modify. The **edit** link is displayed.
2. Click the **edit** link. The edit window for modifying W-IAP details is displayed.
3. Click the **Radio** tab. The **Radio** tab details are displayed.
4. Ensure that an appropriate mode is selected.
5. Select the **Adaptive radio management assigned** option under the bands that are applicable to the W-IAP configuration.
6. Click **OK**.

Configuring Radio Profiles Manually for W-IAP

When radio settings are assigned manually by the administrator, the ARM is disabled.

To manually configure radio settings:

1. In the **Access Points** tab, click the AP for which you want to enable ARM. The **edit** link is displayed.
2. Click the **edit** link. The **Edit Access Point** window is displayed.
3. Click the **Radio** tab.
4. Ensure that an appropriate mode is selected.

   By default the channel and power for an AP are optimized dynamically using Adaptive Radio Management (ARM). You can override ARM on the 2.4 GHz and 5 GHz bands and set the channel and power manually if desired. The following table describes various configuration modes for an AP:

Table 18: *W-IAP Radio Modes*

Mode	Description
Access	In **Access** mode, the AP serves clients, while also monitoring for rogue APs in the background. If the **Access** mode is selected, perform the following actions: 1. Select **Administrator assigned** in **2.4 GHz** and **5 GHz** band sections. 2. Select appropriate channel number from the **Channel** drop-down list for both **2.4 GHz** and **5 GHz** band sections. 3. Enter appropriate transmit power value in the **Transmit power** text box in **2.4 GHz** and **5 GHz** band sections.
Monitor	In **Monitor** mode, the AP acts as a dedicated monitor, scanning all channels for rogue APs and clients. You can set one radio on the Monitor mode and the other radio on access mode, so that the clients can use one radio when the other one is in the Air Monitor mode.
Spectrum Monitor	In **Spectrum Monitor** mode, the AP functions as a dedicated full-spectrum RF monitor, scanning all channels to detect interference, whether from the neighboring APs or from non-WiFi devices such as microwaves and cordless phones.

In the Spectrum Monitor mode, the APs do not provide access services to clients.

4. Click **OK**.

In the CLI

To configure a radio profile:

```
(Instant AP)# wifi0-mode {<access>|<monitor>|<spectrum-monitor>}
(Instant AP)# wifi1-mode {<access>|<monitor>|<spectrum-monitor>}
```

If the access mode is configured, you can configure the channel and transmission power by running the following commands:

```
(Instant AP)# a-channel <channel> <tx-power>
(Instant AP)# g-channel <channel> <tx-power>
```

Configuring Uplink VLAN for a W-IAP

Instant supports a management VLAN for the uplink traffic on a W-IAP. You can configure an uplink VLAN when a W-IAP needs to be managed from a non-native VLAN. After a W-IAP is provisioned with the uplink management VLAN, all management traffic sent from the W-IAP is tagged with the management VLAN.

Ensure that the native VLAN of the W-IAP and uplink are not the same.

You can configure the uplink management VLAN on a W-IAP by using the Instant UI or CLI.

In the Instant UI

To configure uplink management VLAN:

1. In the **Access Points** tab, click the W-IAP to modify. The **edit** link is displayed.

2. Click the **edit** link. The **edit** window for modifying W-IAP details is displayed.
3. Click the **Uplink** tab.
4. Specify the VLAN in the **Uplink Management VLAN** field.
5. Click **OK**.
6. Reboot the W-IAP.

In the CLI

To configure uplink VLAN:

```
(Instant AP)# uplink-vlan <VLAN-ID>
```

To view the uplink VLAN status:

```
(Instant AP)# show uplink-vlan
Uplink Vlan Current :0
Uplink Vlan Provisioned :1
```

Master Election and Virtual Controller

Instant does not require an external mobility controller to regulate and manage the Wi-Fi network. Instead, one W-IAP in every network assumes the role of Virtual Controller. It coordinates, stores, and distributes the settings required to provide a centralized functionality to regulate and manage the Wi-Fi network. The Virtual Controller is the single point of configuration and firmware management. When configured, the Virtual Controller sets up and manages the VPN tunnel to a Mobility Controller in the data center.

The Virtual Controller also functions like any other AP with full RF scalability. It also acts as a node, coordinating DHCP address allocation for network address translated clients ensuring mobility of the clients when they roam between different W-IAPs.

Master Election Protocol

The Master Election Protocol enables the Instant network to dynamically elect a W-IAP to take on a Virtual Controller role and allow graceful failover to a new Virtual Controller when the existing Virtual Controller is not available. This protocol ensures stability of the network during initial startup or when the Virtual Controller goes down by allowing only one W-IAP to self-elect as a Virtual Controller.

Preference to a W-IAP with 3G/4G Card

The Master Election Protocol prefers the W-IAP with a 3G/4G card, when electing a Virtual Controller for the Instant network during the initial setup. The Virtual Controller is selected based on the following criteria:

- If there is more than one W-IAP with 3G/4G cards, one of these W-IAPs is dynamically elected as the Virtual Controller.
- When a W-IAP without 3G/4G card is elected as the Virtual Controller but is up for less than 5 minutes, another W-IAP with 3G/4G card in the network is elected as the Virtual Controller to replace it and the previous Virtual Controller reboots.
- When a W-IAP without 3G/4G card is already elected as the Virtual Controller and is up for more than 5 minutes, the Virtual Controller will not be replaced until it goes down.

W-IAP135 is preferred over W-IAP105 when a Virtual Controller is elected.

Preference to a W-IAP with Non-Default IP

The Master Election Protocol prefers a W-IAP with non-default IP, when electing a Virtual Controller for the Instant network during initial startup. If there are more than one W-IAP with non-default IPs in the network, all W-IAPs with default IP will automatically reboot and the DHCP process is used to assign new IP addresses.

Viewing Master Election Details

To verify the status of a W-IAP and master election details, use the following commands:

```
(Instant AP)# show election statistics
(Instant AP)# show summary support
```

Manual Provisioning of Master W-IAP

In most cases, the master election process automatically determines the best W-IAP that can perform the role of Virtual Controller, which will apply its image and configuration to all other W-IAPs in the same AP management VLAN. When the Virtual Controller goes down, a new Virtual Controller is elected.

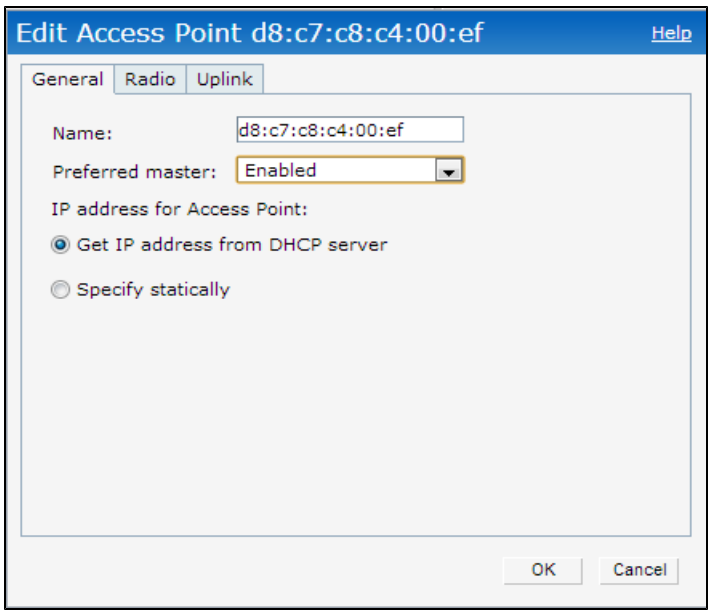
Provisioning a W-IAP as a Master W-IAP

You can provision a W-IAP as a master W-IAP by using the Instant UI or CLI.

In the Instant UI

1. In the **Access Points** tab, click the W-IAP to modify. The **edit** link is displayed.
2. Click the **edit** link. The edit window for modifying W-IAP details is displayed.
3. Select **Enabled** from **Preferred master** drop-down. This option is disabled by default.

Figure 31 *W-IAP Settings—Provisioning Master W-IAP*



4. Click **OK**.

In the CLI

To provision a W-IAP as a master W-IAP:

```
(Instant AP)# iap-master
```

To verify if the W-IAP is provisioned as master IAP:

```
(Instant AP)# show ap-env
Antenna Type:Internal
```

```
Iap_master:1
```

Adding a W-IAP to the Network

To add a W-IAP to the Instant network, assign an IP address. For more information, see Assigning an IP address to the W-IAP on page 35.

After a W-IAP is connected to the network, if the Auto Join Mode feature is enabled, the W-IAP inherits the configuration from the Virtual Controller and is listed in the **Access Points** tab.

If the Auto Join Mode is disabled, perform the following steps to add a W-IAP to the network:

1. In the **Access Points** tab, click the **New** link. The **New Access Point** window is displayed.
2. In the **New Access Point** window, enter the MAC address for the new W-IAP.
3. Click **OK.**

Removing a W-IAP from the Network

You can remove a W-IAP from the network only if the Auto Join Mode feature is disabled. To remove a W-IAP from the network:

1. In the **Access Points** tab, click the W-IAP to delete. The **x** icon is displayed against the W-IAP.
2. Click **x** to confirm the deletion.

The deleted W-IAPs cannot join the Instant network anymore and no longer are displayed in the Instant UI. However, the master W-IAP details cannot be deleted from the Virtual Controller database.

VLAN configuration is required for networks with more devices and broadcast traffic on a WLAN SSID or wired profile. Based on the network type and its requirements, you can configure the VLANs for a WLAN SSID or wired port profile.

For more information on VLAN configuration for a WLAN SSID and wired port profile, see Configuring VLAN Settings for a WLAN SSID Profile on page 97 and Configuring VLAN for a Wired Profile on page 114.

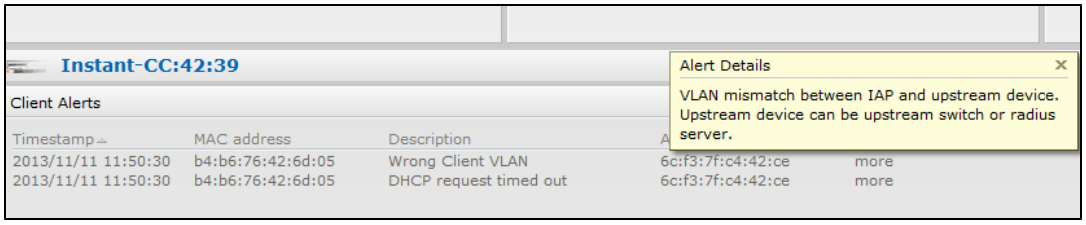
VLAN Pooling

In a single W-IAP cluster, a large number of clients can be assigned to the same VLAN. Using the same VLAN for multiple clients can lead to a high level of broadcasts in the same subnet. To manage the broadcast traffic, you can partition the network into different subnets and use L3-mobility between those subnets when clients roam. However, if a large number of clients need to be in the same subnet, you can configure VLAN pooling, in which each client is randomly assigned a VLAN from a pool of VLANs on the same SSID. Thus, VLAN pooling allows automatic partitioning of a single broadcast domain of clients into multiple VLANs.

Uplink VLAN Monitoring and Detection on Upstream Devices

If a client connects to an SSID or wired interface with a VLAN that is not allowed on the upstream device, the client will not be assigned an IP address and thus cannot connect to the Internet. When a client connects to an SSID or a wired interface with VLAN that is not allowed on the upstream device, the Instant UI now displays the following alert message:

Figure 32 *Uplink VLAN Detection*



To resolve this issue, ensure that there is no mismatch in the VLAN configuration.

This chapter provides the following information:

- Configuring Wireless Network Profiles on page 93
- Configuring Fast Roaming for Wireless Clients on page 106
- Editing Status of a WLAN SSID Profile on page 110
- Editing a WLAN SSID Profile on page 110
- Deleting a WLAN SSID Profile on page 111

Configuring Wireless Network Profiles

During start up, a wireless client searches for radio signals or beacon frames that originate from the nearest W-IAP. After locating the W-IAP, the following transactions take place between the client and the W-IAP:

1. Authentication – The W-IAP communicates with a RADIUS server to validate or authenticate the client.
2. Connection – After successful authentication, the client establishes a connection with the W-IAP.

Network Types

Instant wireless networks are categorized as:

- **Employee network** – An Employee network is a classic Wi-Fi network. This network type is used by the employees in an organization and it supports passphrase-based or 802.1X based authentication methods. Employees can access the protected data of an enterprise through the employee network after successful authentication. The employee network is selected by default during a network profile configuration.
- **Voice network** –This Voice network type allows you to configure a network profile for devices that provide only voice services such as handsets or applications that require voice traffic prioritization.
- **Guest network** –The Guest wireless network is created for guests, visitors, contractors, and any non-employee users who use the enterprise Wi-Fi network. The Virtual Controller assigns the IP address for the guest clients. captive portal or passphrase based authentication methods can be set for this wireless network. Typically, a guest network is an un-encrypted network. However, you can specify the encryption settings when configuring a guest network.

When a client is associated to the Voice network, all data traffic is marked and placed into the high priority queue in QoS (Quality of Service).

To configure a new wireless network profile, complete the following procedures:

1. Configuring WLAN Settings
2. Configuring VLAN Settings
3. Configuring Security Settings
4. Configuring Access Rules for a Network

Configuring WLAN Settings for an SSID Profile

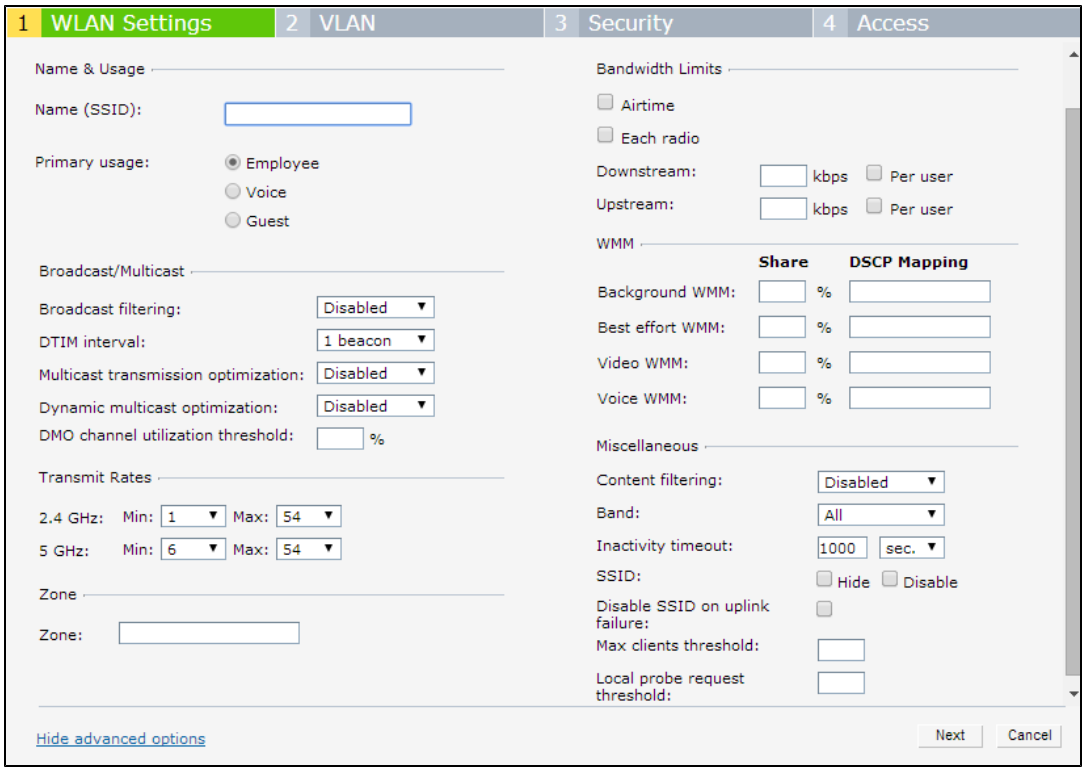
You can configure WLAN settings using the Instant UI or CLI.

In the Instant UI

To configure WLAN settings:

1. In the **Networks** tab of the Instant main window, click the **New** link. The **New WLAN** window is displayed. The following figure shows the contents of the **WLAN Settings** tab:

Figure 33 *WLAN Settings Tab*



2. Enter a name that uniquely identifies a wireless network in the **Name (SSID)** text box.

The SSID Name may contain any special character except for ' and ".

3. Based on the type of network profile, select any of the following options under **Primary usage**:
   - **Employee**
   - **Voice**
   - **Guest**
4. Click the **Show advanced options** link. The advanced options for configuration are displayed. Specify the following parameters as required.

Table 19: *WLAN Configuration Parameters*

Parameter	Description
Broadcast filtering	Select any of the following values: • **All**–When set to **All**, the W-IAP drops all broadcast and multicast frames except DHCP and ARP. • **ARP**–When set to **ARP**, the W-IAP converts ARP requests to unicast and send frames directly to the associated client. • **Disabled**– When set to **Disabled**, all broadcast and multicast traffic is forwarded.
DTIM interval	The **DTIM interval** indicates the delivery traffic indication message (DTIM) period in beacons, which can be configured for every WLAN SSID profile. The DTIM interval determines how often the W-IAP should deliver the buffered broadcast and multicast frames to associated clients in the powersave mode. The default value is 1, which means the client checks for buffered data on the W-IAP at every beacon. You can also configure a higher DTIM value for power saving.
Multicast transmission optimization	Select **Enabled** if you want the W-IAP to select the optimal rate for sending broadcast and multicast frames based on the lowest of unicast rates across all associated clients. When this option is enabled, multicast traffic can be sent at up to 24 Mbps. The default rate for sending frames for 2.4 GHz is 1 Mbps and 5.0 GHz is 6 Mbps. This option is disabled by default.
Dynamic multicast optimization	Select **Enabled** to allow W-IAP to convert multicast streams into unicast streams over the wireless link. Enabling Dynamic Multicast Optimization (DMO) enhances the quality and reliability of streaming video, while preserving the bandwidth available to the non-video clients. **NOTE:** When you enable DMO on multicast SSID profiles, ensure that the DMO feature is enabled on all SSIDs configured in the same VLAN.
DMO channel utilization threshold	Specify a value to set a threshold for DMO channel utilization. With DMO, the W-IAP converts multicast streams into unicast streams as long as the channel utilization does not exceed this threshold. The default value is 90% and the maximum threshold value is 100%. When the threshold is reached or exceeds the maximum value, the W-IAP sends multicast traffic over the wireless link.
Transmit Rates	Specify the following parameters: • **2.4 GHz**–If the 2.4 GHz band is configured on the W-IAP, specify the minimum and maximum transmission rate. The default value for minimum transmission rate is 1 Mbps and maximum transmission rate is 54 Mbps. • **5 GHz**–If the 5 GHz band is configured on the W-IAP, specify the minimum and maximum transmission rate. The default value for minimum transmission rate is 6 Mbps and maximum transmission rate is 54 Mbps.
Zone	Specify the zone for the SSID. When the zone is defined in SSID profile and if the same zone is defined on a W-IAP, the SSID is created on that W-IAP. For more information on configuring zone details on an IAP, see Configuring Zone Settings on a W-IAP on page 84. The following constraints apply to the zone configuration: • A W-IAP can belong to only one zone and only one zone can be configured on an SSID. • If an SSID belongs to a zone, all W-IAPs in this zone can broadcast this SSID. If no W-IAP belongs to the zone configured on the SSID, the SSID is not broadcast. • If an SSID does not belong to any zone, all W-IAPs can broadcast this SSID.
Bandwidth Limits	Under **Bandwidth Limits**: • **Airtime**–Select this checkbox to specify an aggregate amount of airtime that all clients in this network can use for sending and receiving data. Specify the airtime percentage. • **Each radio**– Select this checkbox to specify an aggregate amount of throughput that each radio is allowed to provide for the connected clients. • **Downstream** and **Upstream**–Specify the downstream and upstream rates within a range of 1 to 65535 Kbps for the SSID users. If the assignment is specific for each user, select the **Peruser** checkbox.

Table 19: *WLAN Configuration Parameters*

Parameter	Description
Wi-Fi Multimedia (WMM) traffic management	Configure the following options for WMM traffic management. WMM supports voice, video, best effort, and background access categories. To allocate bandwidth for the following types of traffic, specify a percentage value under **Share**. To configure DSCP mapping, specify a value under **DSCP Mapping**. • **Background WMM**: For background traffic such as file downloads or print jobs. • **Best effort WMM** – For best effort traffic such as traffic from legacy devices or traffic from applications or devices that do not support QoS. • **Video WMM** – For video traffic generated from video streaming. • **Voice WMM**– For voice traffic generated from the incoming and outgoing voice communication. For more information on WMM traffic and DSCP mapping, see Wi-Fi Multimedia Traffic Management on page 251
Content filtering	Select **Enabled** to route all DNS requests for the non-corporate domains to OpenDNS on this network.
Band	Select a value to specify the band at which the network transmits radio signals. You can set the band to **2.4 GHz**, **5 GHz**, or **All**. The **All** option is selected by default.
Inactivity timeout	Specify an interval for session timeout in seconds, minutes or hours. If a client session is inactive for the specified duration, the session expires and the users are required to log in again. You can specify a value within the range of 60-86400 seconds or up to 24 hours for a client session. The default value is 1000 seconds.
Hide SSID	Select this checkbox if you do not want the SSID (network name) to be visible to users.
Disable SSID	Select this checkbox if you want to disable the SSID. On selecting this, the SSID will be disabled, but will not be removed from the network. By default, all SSIDs are enabled.
Can be used without Uplink	Select the checkbox if you do not want to SSID profile to use uplink.
Max clients threshold	Specify the maximum number of clients that can be configured for each BSSID on a WLAN. You can specify a value within the range of 0 to 255. The default value is 64.
Local probe request threshold	Specify a threshold value to limit the number of incoming probe requests. When a client sends a broadcast probe request frame to search for all available SSIDs, this option controls system response for this network profile and ignores probe requests if required. You can specify a Received signal strength indication (RSSI) value within range of 0 to 100 dB.

5. Click **Next** to configure VLAN settings. For more information, see Configuring VLAN Settings for a WLAN SSID Profile on page 97.

In the CLI

To configure WLAN settings for an SSID profile:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# essid <ESSID-name>
(Instant AP)(SSID Profile <name>)# type {<Employee>|<Voice>| <Guest>}
(Instant AP)(SSID Profile <name>)# broadcast-filter <type>
(Instant AP)(SSID Profile <name>)# dtim-period <number-of-beacons>
(Instant AP)(SSID Profile <name>)# multicast-rate-optimization
(Instant AP)(SSID Profile <name>)# dynamic-multicast-optimization
(Instant AP)(SSID Profile <name>)# dmo-channel-utilization-threshold
(Instant AP)(SSID Profile <name>)# a-max-tx-rate <rate>
(Instant AP)(SSID Profile <name>)# a-min-tx-rate <rate>
(Instant AP)(SSID Profile <name>)# g-max-tx-rate <rate>
(Instant AP)(SSID Profile <name>)# g-min-tx-rate <rate>
```

```
(Instant AP)(SSID Profile <name>)# zone <zone>
(Instant AP)(SSID Profile <name>)# bandwidth-limit <limit>
(Instant AP)(SSID Profile <name>)# per-user-bandwidth-limit <limit>
(Instant AP)(SSID Profile <name>)# air-time-limit <limit>
(Instant AP)(SSID Profile <name>)# wmm-background-dscp <dscp>
(Instant AP)(SSID Profile <name>)# wmm-background-share <share>
(Instant AP)(SSID Profile <name>)# wmm-best-effort-dscp <dscp>
(Instant AP)(SSID Profile <name>)# wmm-best-effort-share <share>
(Instant AP)(SSID Profile <name>)# wmm-video-dscp <dscp>
(Instant AP)(SSID Profile <name>)# wmm-video-share <share>
(Instant AP)(SSID Profile <name>)# wmm-voice-dscp <dscp>
(Instant AP)(SSID Profile <name>)# wmm-voice-share <share>
(Instant AP)(SSID Profile <name>)# rf-band {<2.4>|<5.0>|<all>}
(Instant AP)(SSID Profile <name>)# content-filtering
(Instant AP)(SSID Profile <name>)# hide-ssid
(Instant AP)(SSID Profile <name>)# inactivity-timeout <interval>
(Instant AP)(SSID Profile <name>)# work-without-uplink
(Instant AP)(SSID Profile <name>)# local-probe-req-thresh <threshold>
(Instant AP)(SSID Profile <name>)# max-clients-threshold <number-of-clients>
(Instant AP)(SSID Profile <name>)# end
(Instant AP)# commit apply
```

Configuring VLAN Settings for a WLAN SSID Profile

If you are creating a new SSID profile, complete the WLAN Settings procedure before configuring VLAN. For more information, see Configuring WLAN Settings for an SSID Profile on page 93.

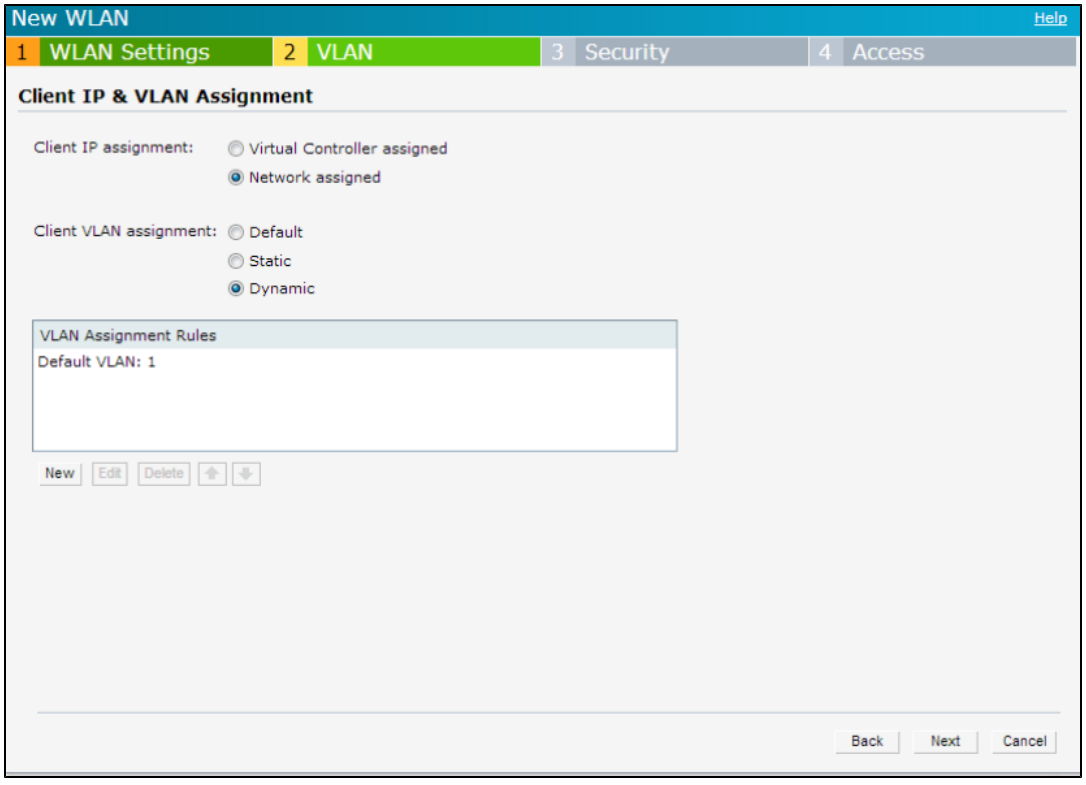
You can configure VLAN settings for an SSID profile using the Instant UI or CLI.

In the Instant UI

To configure VLAN settings for an SSID:

1. In the **VLAN** tab of the **New WLAN** window. The VLAN tab contents are displayed.

Figure 34 *VLAN Tab*



2. Select any for the following options for **Client IP assignment**:
   - **Virtual Controller assigned**–On selecting this option, the client obtains the IP address from the Virtual Controller.
   - **Network assigned**–On selecting this option, the IP address is obtained from the network.
3. Based on the type client IP assignment mode selected, you can configure the VLAN assignment for clients as described in the following table:

Table 20: *IP and VLAN Assignment for WLAN SSID Clients*

Client IP Assignment	Client VLAN Assignment
Virtual Controller assigned	If the **Virtual Controller assigned** is selected for client IP assignment, the Virtual Controller creates a private subnet and VLAN on the W-IAP for the wireless clients. The network address translation for all client traffic that goes out of this interface is carried out at the source. This setup eliminates the need for complex VLAN and IP address management for a multi-site wireless network. On selecting this option, the following client VLAN assignment options are displayed: • **Default**: When selected, the default VLAN as determined by the Virtual Controller is assigned for clients. • **Custom**: When selected, you can specify a custom VLAN assignment option. You can select an existing DHCP scope for client IP and VLAN assignment or you can create a new DHCP scope by selecting **New**. For more information on DHCP scopes, see Configuring DHCP Scopes on page 201.

Network assigned	If the **Network assigned** is selected, you can specify any of the following options for the **Client VLAN assignment**.
	• **Default**– On selecting this option, the client obtains the IP address in the same subnet as the W-IAPs. By default, the client VLAN is assigned to the native VLAN on the wired network.
	• **Static**– On selecting this option, you need to specify a single VLAN, a comma separated list of VLANS, or a range of VLANs for all clients on this network. Select this option for configuring VLAN pooling.
	• **Dynamic**– On selecting this option, you can assign the VLANs dynamically from a Dynamic Host Configuration Protocol (DHCP) server. To create VLAN assignment rules, click **New** to assign the user to a VLAN. In the **New VLAN Assignment Rule** window, enter the following information:
	  • **Attribute**– Select an attribute returned by the RADIUS server during authentication.
	  • **Operator**– Select an operator for matching the string.
	  • **String**– Enter the string to match
	  • **VLAN**– Enter the VLAN to be assigned.

4. Click **Next** to configure security settings for the employee network. For more information, see Configuring Security Settings for a WLAN SSID Profile on page 99.

In the CLI

To manually assign VLANs for WLAN SSID users:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# vlan <vlan-ID>
(Instant AP)(SSID Profile <name>)# end
(Instant AP)# commit apply
```

To enforce DHCP-based VLAN assignment:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# enforce-dhcp
(Instant AP)(SSID Profile <name>)# end
```

```
(Instant AP)# commit apply
```

To create a new VLAN assignment rule:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# set-vlan <attribute> {{contains|ends-with|equals|matches-regular-expression|not-equals|starts-with} <operand> <vlan>|value-of}
(Instant AP)(SSID Profile <name>)# end
(Instant AP)# commit apply
```

Configuring Security Settings for a WLAN SSID Profile

The following procedures are described in this section:

- Configuring Security Settings for an Employee or Voice Network on page 99

For information on guest network configuration, see Captive Portal for Guest Access.

If you are creating a new SSID profile, configure the WLAN and VLAN settings before defining security settings. For more information, see Configuring WLAN Settings for an SSID Profile on page 93 and Configuring VLAN Settings for a WLAN SSID Profile on page 97.

Configuring Security Settings for an Employee or Voice Network

You can configure security settings for an employee or voice network by using the Instant UI or CLI.

In the Instant UI

To configure security settings for an employee or voice network:

1. In the **Security** tab, specify any of the following types of security levels by moving the slider to a desired level:
   - **Enterprise**–On selecting enterprise security level, the authentication options applicable to the enterprise network are displayed.
   - **Personal** – On selecting personal security level, the authentication options applicable to the personalized network are displayed.
   - **Open**–On selecting Open security level, the authentication options applicable to an open network are displayed:

   The default security setting for a network profile is **Personal**.

   The following figures show the configuration options for **Enterprise**, **Personal**, and **Open** security settings:

Figure 35 *Security Tab: Enterprise*

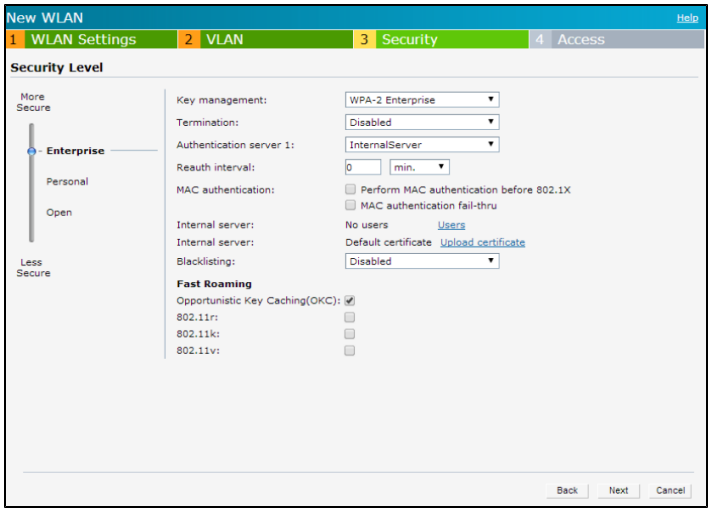


Figure 36 *Security Tab: Personal*

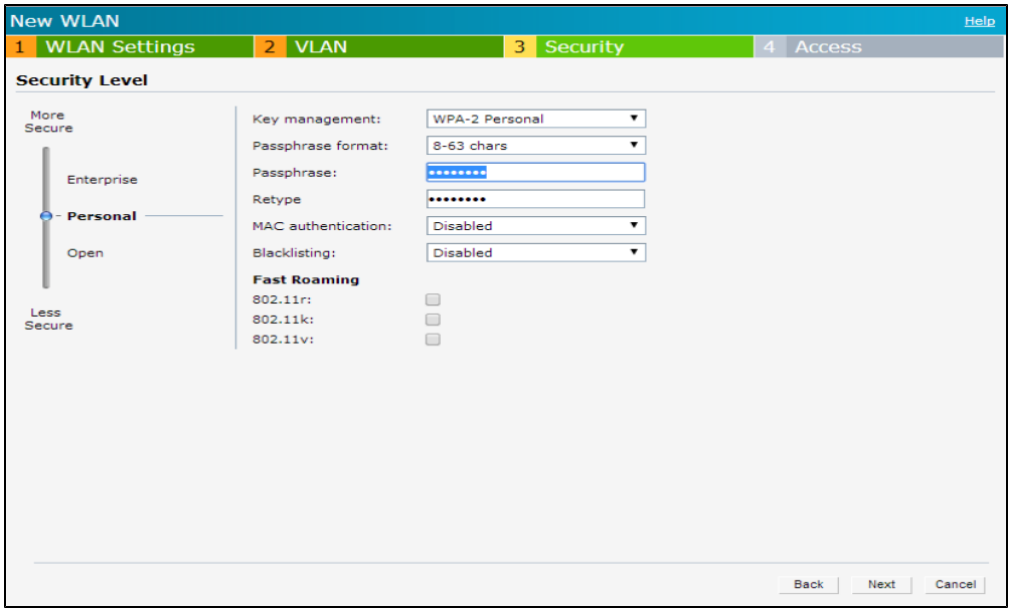
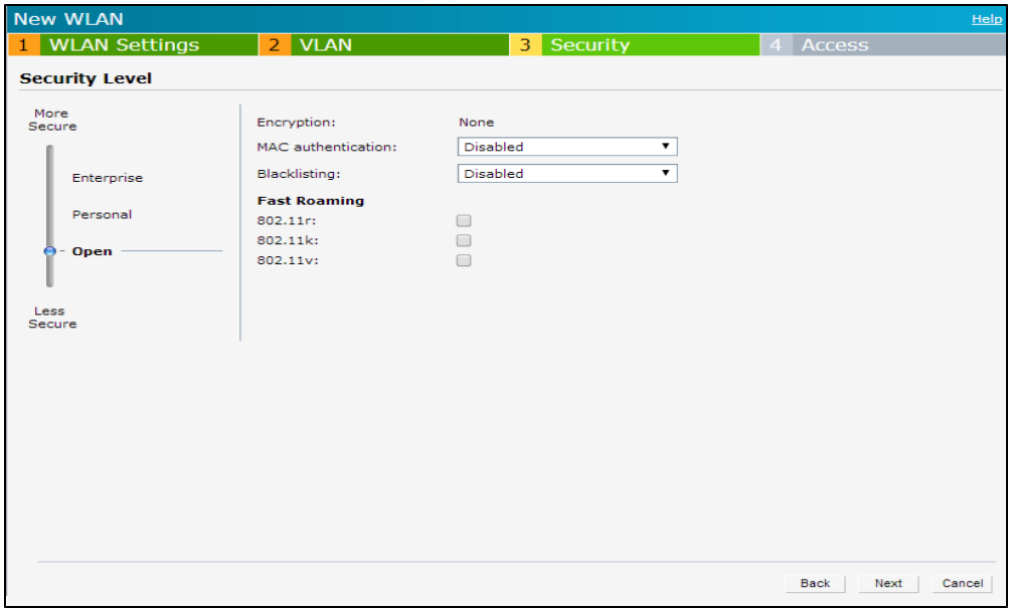


Figure 37 *Security Tab: Open*



2. Based on the security level specified, specify the following parameters:

Table 21: *Configuration Parameters for WLAN Security Settings in an Employee or Voice Network*

Parameter	Description	Security Level Type
Key Management	For **Enterprise** security level, select any of the following options from the **Key management** drop-down list: • WPA-2 Enterprise • Both (WPA-2 & WPA) • WPA Enterprise • Dynamic WEP with 802.1X – If you do not want to use a session key from the RADIUS Server to derive pair wise unicast keys, set **Session Key for LEAP** to **Enabled**. This is required for old printers that use dynamic WEP through Lightweight Extensible Authentication Protocol (LEAP) authentication. The **Session Key for LEAP** feature is **Disabled** by default.	Applicable to **Enterprise** and **Personal** security levels only. For the **Open** security level, no encryption settings are required.
	For **Personal** security level, select an encryption key from the **Key management** drop-down list. • For WPA-2 Personal, WPA Personal, and Both (WPA-2&WPA) keys, specify the following parameters: 1. **Passphrase format**: Select a passphrase format from the **Passphrase format** drop-down list. The options are available are 8-63 alphanumeric characters and 64 hexadecimal characters. 2. Enter a passphrase in the **Passphrase** text box and reconfirm. **NOTE:** The **Passphrase** may contain any special character except for **"**. • For **Static WEP**, specify the following parameters: 1. Select an appropriate value for **WEP key size** from the WEP key size drop-down list. You can specify 64-bit or 128-bit . 2. Select an appropriate value for Tx key from the **Tx Key** drop-down list. You can specify **1**, **2**, **3**, or **4**. 3. Enter an appropriate **WEP key** and reconfirm.	
Termination	To terminate the EAP portion of 802.1X authentication on the W-IAP instead of the RADIUS server, set **Termination** to **Enabled**. Enabling **Termination** can reduce network traffic to the external RADIUS server by terminating the authorization protocol on the W-IAP. By default, for 802.1X authorization, the client conducts an EAP exchange with the RADIUS server, and the W-IAP acts as a relay for this exchange. When **Termination** is enabled, the W-IAP by itself acts as an authentication server and terminates the outer layers of the EAP protocol, only relaying the innermost layer to the external RADIUS server. It can also reduce the number of exchange packets between the W-IAP and authentication server. **NOTE:** Instant supports the configuration of primary and backup authentication servers in an EAP termination enabled SSID. **NOTE:** If you are using LDAP for authentication, ensure that AP termination is configured to support EAP.	**Enterprise** security level
Authentication server 1 and **Authentication server 2**	Select any of the following options from the **Authentication server 1** drop-down list: • Select an authentication server from the list if an external servers are already configured. • Select **New** to configure any of the following servers as an external server:	**Enterprise**, **Personal**, and **Open** security levels.

Table 21: *Configuration Parameters for WLAN Security Settings in an Employee or Voice Network*

Parameter	Description	Security Level Type
	• RADIUS Server • LDAP Server • CPPM Server for AirGroup **CoA** For information on configuring external servers, see Configuring an External Server for Authentication on page 157. • To use an internal server, select **Internal server** and add the clients that are required to authenticate with the internal RADIUS server. Click the **Users** link to add the users. For information on adding a user, see Managing W-IAP Users on page 140. If an external server is selected, you can also configure another authentication server.	
Load balancing	Set this to **Enabled** if you are using two RADIUS authentication servers, so that the load across the two RADIUS servers is balanced. For more information on the dynamic load balancing mechanism, see Dynamic Load Balancing between Two Authentication Servers on page 154.	**Enterprise**, **Personal**, and **Open** security levels.
Reauth interval	Specify a value for **Reauth interval**. When set to a value greater than zero, APs periodically reauthenticate all associated and authenticated clients.	**Enterprise**, **Personal**, and **Open** security levels.
Blacklisting	To enable blacklisting of the clients with a specific number of authentication failures, select **Enabled** from the **Blacklisting** drop-down list and specify a value for **Max authentication failures**. The users who fail to authenticate the number of times specified in **Max authentication failures** field are dynamically blacklisted.	**Enterprise**, **Personal**, and **Open** security levels.
Accounting	To enable accounting, select **Enabled** from the **Accounting** drop-down list. On setting this option to **Enabled**, APs post accounting information to the RADIUS server at the specified **Accounting interval**.	**Enterprise**, **Personal**, and **Open** security levels.
Authentication survivability	To enable authentication survivability, set **Authentication survivability** to **Enabled**. Specify a value in hours for **Cache timeout (global)** to set the duration after which the authenticated credentials in the cache must expire. When the cache expires, the clients are required to authenticate again. You can specify a value within range of 1 to 99 hours and the default value is 24 hours. **NOTE:** The authentication survivability feature requires ClearPass Policy Manager 6.0.2 or later, and is available only when the **New** server option is selected authentication. On setting this parameter to **Enabled**, Instant authenticates the previously connected clients using EAP-PEAP authentication even when connectivity to ClearPass Policy Manager is temporarily lost. The Authentication survivability feature is not applicable when a RADIUS server is configured as an internal server.	**Enterprise** security level
MAC authentication	To enable MAC address based authentication for **Personal** and **Open** security levels, set **MAC authentication** to **Enabled**. For **Enterprise** security level, the following options are available: • **Perform MAC authentication before 802.1X** – Select this checkbox to use 802.1X authentication only when the MAC authentication is successful. • **MAC authentication fail-thru** – On selecting this checkbox, the 802.1X authentication is attempted when the MAC authentication fails.	**Enterprise**, **Personal**, and **Open** security levels.

Table 21: *Configuration Parameters for WLAN Security Settings in an Employee or Voice Network*

Parameter	Description	Security Level Type
Delimiter character	Specify a character (for example, colon or dash) as a delimiter for the MAC address string. When configured, the W-IAP will use the delimiter in the MAC authentication request. For example, if you specify the colon as a delimiter, MAC addresses in the xx:xx:xx:xx:xx:xx format are used. If the delimiter is not specified, the MAC address in the xxxxxxxxxxxx format is used. This option is available only when MAC authentication is enabled.	**Enterprise**, **Personal**, and **Open** security levels.
Uppercase support	Set to **Enabled** to allow the W-IAP to use uppercase letters in MAC address string for MAC authentication. This option is available only if MAC authentication is enabled.	**Enterprise**, **Personal**, and **Open** security levels.
Upload Certificate	Click **Upload Certificate** and browse to upload a certificate file for the internal server. For more information on certificates, see Uploading Certificates on page 173.	**Enterprise**, **Personal**, and **Open** security levels
Fast Roaming	You can configure the following fast roaming options for the WLAN SSID: • **Opportunistic Key Caching**: When **WPA-2 Enterprise** and **Both (WPA2-WPA)** encryption types are selected and if 802.1x authentication method is configured, the **Opportunistic Key Caching** (OKC) is enabled by default. If OKC is enabled, a cached pairwise master key (PMK) is used when the client roams to a new AP. This allows faster roaming of clients without the need for a complete 802.1x authentication. • **802.11r**: Selecting this checkbox enables fast BSS transition. The Fast BSS Transition mechanism minimizes the delay when a client transitions from one BSS to another within the same cluster. • **802.11k**: Selecting this checkbox enables 802.11k roaming on the SSID profile. The 802.11k protocol enables W-IAPs and clients to dynamically measure the available radio resources. When 802.11k is enabled, W-IAPs and clients send neighbor reports, beacon reports, and link measurement reports to each other. • **802.11v**: Selecting this checkbox enables 802.11v based BSS transition.802.11v standard defines mechanisms for wireless network management enhancements and BSS transition management. It allows the client devices to exchange information about the network topology and RF environment. The BSS transition management mechanism enables an AP to request a voice client to transition to a specific AP, or suggest a set of preferred APs to a voice client, due to network load balancing or BSS termination. It also helps the voice client identify the best AP to transition to as they roam.	**Enterprise**, **Personal**, and **Open** security levels. **NOTE:** OKC roaming can be configured only for the **Enterprise** security level.

4. Click **Next** to configure access rules. For more information, see Configuring Access Rules for a WLAN SSID Profile on page 104.

In the CLI

To configure enterprise security settings for the employee and voice users of a WLAN SSID profile:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# opmode {wpa2-aes|wpa-tkip,wpa2-aes|wpa-psk-tkip,wpa2-psk-aes|dynamic-wep}
(Instant AP)(SSID Profile <name>)# leap-use-session-key
(Instant AP)(SSID Profile <name>)# termination
(Instant AP)(SSID Profile <name>)# auth-server <server-name>
(Instant AP)(SSID Profile <name>)# external-server
(Instant AP)(SSID Profile <name>)# server-load-balancing
```

```
(Instant AP)(SSID Profile <name>)# blacklist
(Instant AP)(SSID Profile <name>)# mac-authentication
(Instant AP)(SSID Profile <name>)# l2-auth-failthrough
(Instant AP)(SSID Profile <name>)# auth-survivability
(Instant AP)(SSID Profile <name>)# radius-accounting
(Instant AP)(SSID Profile <name>)# radius-accounting-mode {user-association| user-
authentication}
(Instant AP)(SSID Profile <name>)# radius-interim-accounting-interval <minutes>
(Instant AP)(SSID Profile <name>)# radius-reauth-interval <minutes>
(Instant AP)(SSID Profile <name>)# max-authentication-failures <number>
(Instant AP)(SSID Profile <name>)# no okc-disable
(Instant AP)(SSID Profile <name>)# dot11r
(Instant AP)(SSID Profile <name>)# dot11k
(Instant AP)(SSID Profile <name>)# dot11v
(Instant AP)(SSID Profile <name>)# exit
(Instant AP)(config)# auth-survivability cache-time-out
(Instant AP)(config)# end
(Instant AP)# commit apply
```

To configure personal security settings for the employee and voice users of a WLAN SSID profile:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# opmode {wpa2-psk-aes|wpa-tkip| wpa-psk-tkip|wpa-psk-
tkip,wpa2-psk-aes| static-wep}
(Instant AP)(SSID Profile <name>)# mac-authentication
(Instant AP)(SSID Profile <name>)# auth-server <server-name>
(Instant AP)(SSID Profile <name>)# external-server
(Instant AP)(SSID Profile <name>)# server-load-balancing
(Instant AP)(SSID Profile <name>)# blacklist
(Instant AP)(SSID Profile <name>)# max-authentication-failures <number>
(Instant AP)(SSID Profile <name>)# radius-accounting
(Instant AP)(SSID Profile <name>)# radius-accounting-mode {user-association|user-
authentication}
(Instant AP)(SSID Profile <name>)# radius-interim-accounting-interval <minutes>
(Instant AP)(SSID Profile <name>)# radius-reauth-interval <minutes>
(Instant AP)(SSID Profile <name>)# end
(Instant AP)# commit apply
```

To configure open security settings for employee and voice users of a WLAN SSID profile:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# opmode opensystem
(Instant AP)(SSID Profile <name>)# mac-authentication
(Instant AP)(SSID Profile <name># auth-server <server-name>
(Instant AP)(SSID Profile <name># external-server
(Instant AP)(SSID Profile <name># server-load-balancing
(Instant AP)(SSID Profile <name># blacklist
(Instant AP)(SSID Profile <name># max-authentication-failures <number>
(Instant AP)(SSID Profile <name># radius-accounting
(Instant AP)(SSID Profile <name># radius-accounting-mode {user-association|user-
authentication}
(Instant AP)(SSID Profile <name># radius-interim-accounting-interval <minutes>
(Instant AP)(SSID Profile <name># radius-reauth-interval <minutes>
(Instant AP)(SSID Profile <name># end
(Instant AP)# commit apply
```

Configuring Access Rules for a WLAN SSID Profile

This section describes the procedure for configuring security settings for employee and voice network only. For information on guest network configuration, see Captive Portal for Guest Access.

If you are creating a new SSID profile, complete the WLAN Settings and configure VLAN and security parameters,

before defining access rules. For more information, see Configuring WLAN Settings for an SSID Profile on page 93, Configuring VLAN Settings for a WLAN SSID Profile on page 97, and Configuring Security Settings for a WLAN SSID Profile on page 99.

You can configure up to 128 access rules for an employee, voice , or guest network using the Instant UI or CLI.

In the Instant UI

To configure access rules for an employee or voice network:

1. In the **Access Rules** tab, set slider to any of the following types of access control:
   - **Unrestricted**– Select this to set unrestricted access to the network.
   - **Network-based**– Set the slider to **Network-based** to set common rules for all users in a network. The **Allow any to all destinations** access rule is enabled by default. This rule allows traffic to all destinations. To define an access rule:
     a. Click **New**.
     b. Select appropriate options in the **New Rule** window.
     c. Click **OK**.
   - **Role-based**– Select **Role-based** to enable access based on user roles. For role-based access control:
     - Create a user role if required. For more information, see Configuring User Roles.
     - Create access rules for a specific user role. For more information, see Configuring Access Rules for Network Services on page 177. You can also configure an access rule to enforce captive portal authentication for an SSID that is configured to use 802.1X authentication method. For more information, see Configuring Captive Portal Roles for an SSID on page 135.
     - Create a role assignment rule. For more information, see Configuring Derivation Rules on page 192.
2. Click **Finish**.

In the CLI

To configure access control rules for a WLAN SSID:

```
(Instant AP)(config)# wlan access-rule <name>
(Instant AP)(Access Rule <name>)# rule <dest> <mask> <match> {<protocol> <start-port> <end-port> {permit|deny|src-nat|dst-nat{<IP-address> <port>| <port>}}| app <app> {permit| deny}| appcategory <appgrp>| webcategory <webgrp> {permit| deny}| webreputation <webrep> [<option1....option9>]
(Instant AP)(Access Rule <name>)# end
(Instant AP)# commit apply
```

To configure access control based on the SSID:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# set-role-by-ssid
(Instant AP)(SSID Profile <name>)# end
(Instant AP)# commit apply
```

To configure role assignment rules:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# set-role <attribute>{{equals|not-equals|starts-with|ends-with|contains|matches-regular-expression}<operator><role>|value-of}
(Instant AP)(SSID Profile <name>)# end
(Instant AP)# commit apply
```

To configure a pre-authentication role:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# set-role-pre-auth <pre-authentication-role>
```

```
(Instant AP)(SSID Profile <name>)# end
(Instant AP)# commit apply
```

To configure machine and user authentication roles

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# set-role-machine-auth <machine-authentication-only> <user-authentication-only>
(Instant AP)(SSID Profile <name>)# end
(Instant AP)# commit apply
```

To configure unrestricted access:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# set-role-unrestricted
(Instant AP)(SSID Profile <name>)# end
(Instant AP)# commit apply
```

Example

The following example configures access rules for the wireless network:

```
(Instant AP)(config)# wlan access-rule WirelessRule
(Instant AP)(Access Rule "WirelessRule")# rule 192.0.2.2 255.255.255.0 match 6 4343 4343 log classify-media
(Instant AP)(Access Rule "WirelessRule")# rule any any match app deny throttle-downstream 256 throttle-up 256
(Instant AP)(Access Rule "WirelessRule")# rule any any match appcategory collaboration permit
(Instant AP)(Access Rule "WirelessRule")# rule any any match webcategory gambling deny
(Instant AP)(Access Rule "WirelessRule")# rule any any match webcategory training-and-tools permit
(Instant AP)(Access Rule "WirelessRule")# rule any any match webreputation well-known-sites permit
(Instant AP)(Access Rule "WirelessRule")# rule any any match webreputation safe-sites permit
(Instant AP)(Access Rule "WirelessRule")# rule any any match webreputation benign-sites permit
(Instant AP)(Access Rule "WirelessRule")# rule any any match webreputation suspicious-sites deny
(Instant AP)(Access Rule "WirelessRule")# rule any any match webreputation high-risk-sites deny
(Instant AP)(Access Rule "WirelessRule")# end
(Instant AP)# commit apply
```

Configuring Fast Roaming for Wireless Clients

Instant supports the following features that enable fast roaming of clients:

- Opportunistic Key Caching
- Fast BSS Transition (802.11r Roaming)
- Radio Resource Management (802.11k)
- BSS Transition Management (802.11v)

Opportunistic Key Caching

Instant now supports opportunistic key caching (OKC) based roaming. In the OKC based roaming, the AP stores one pairwise master key (PMK) per client, which is derived from last 802.1x authentication completed by the client in the network. The cached PMK is used when a client roams to a new AP. This allows faster roaming of clients between the W-IAPs in a cluster, without requiring a complete 802.1X authentication.

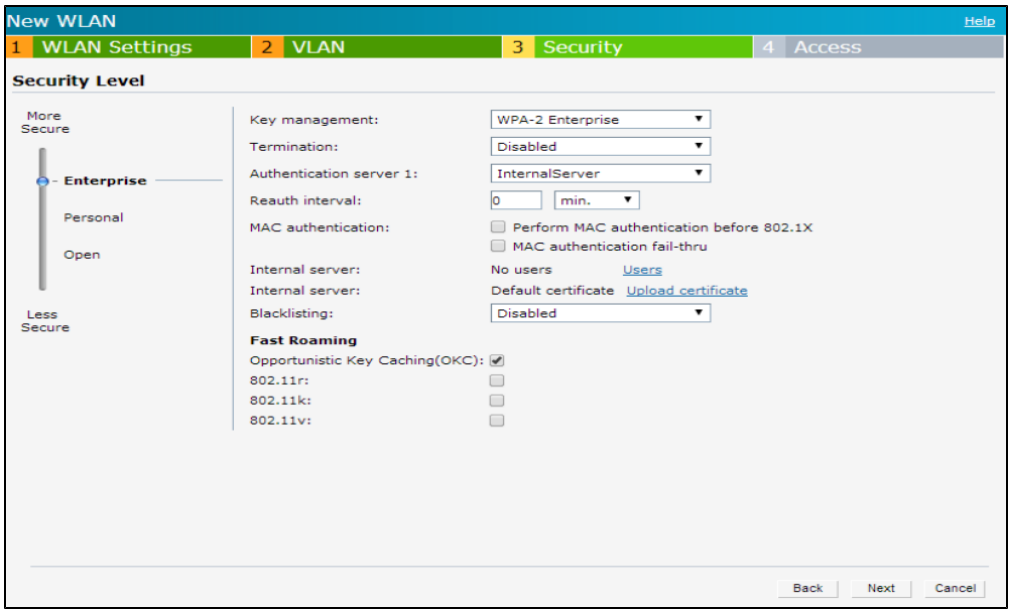
OKC roaming (when configured in the 802.1x Authentication profile) is supported on WPA2 clients. If the wireless client (the 802.1X supplicant) does not support this feature, a complete 802.1X authentication is required whenever a client roams to a new AP.

Configuring a W-IAP for OKC Roaming

You can enable OKC roaming for WLAN SSID by using Instant UI or CLI.

In the Instant UI

1. Navigate to the WLAN wizard (click **Network**>**New** or **Network**> Select the WLAN SSID>**edit**).
2. Click the **Security** tab.
3. Slide to **Enterprise** security level. On selecting a security level, the authentication options applicable to Enterprise network are displayed.



4. Select the **WPA-2 Enterprise** or **Both (WPA-2 & WPA)** option from the **Key management** drop-down list. When any of these encryption types is selected, **Opportunistic Key Caching** (OKC) is enabled by default.
5. Click **Next** and then click **Finish**.

In the CLI

To disable OKC roaming on a WLAN SSID:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# opmode {wpa2-aes|wpa-tkip,wpa-aes,wpa2-tkip,wpa2-aes}
(Instant AP)(SSID Profile <name>)# okc-disable
(Instant AP)(config)# end
(Instant AP)# commit apply
```

To enable OKC roaming on a WLAN SSID:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# opmode {wpa2-aes| wpa-tkip,wpa-aes,wpa2-tkip,wpa2-aes}
(Instant AP)(SSID Profile <name>)# no okc-disable
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Fast BSS Transition (802.11r Roaming)

802.11r is a roaming standard defined by IEEE. When enabled, 802.11r reduces roaming delay by pre-authenticating clients with multiple target APs before a client roams to an AP. With 802.11r implementation, clients pre-authenticate with multiple APs in a cluster.

As part of the 802.11r implementation, Instant supports the Fast BSS Transition protocol. The Fast BSS Transition mechanism reduces client roaming delay when a client transitions from one BSS to another within the same cluster. This minimizes the time required to resume data connectivity when a BSS transition happens.

Fast BSS Transition is operational only if the wireless client supports 802.11r standard. If the client does not support 802.11r standard, it falls back to the normal WPA2 authentication method.

Configuring a W-IAP for 802.11r support

You can configure 802.11r support for a WLAN SSID by using the Instant UI or CLI.

In the Instant UI

1. Navigate to the WLAN wizard (click **Network**>**New** or **Network**> Select the WLAN SSID>**edit**).
2. Click the **Security** tab.
3. Under **Fast Roaming**, select the **802.11r** checkbox.
4. Click **Next** and then click **Finish**.

In the CLI

To enable 802.11r roaming on a WLAN SSID:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# dot11r
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Example

```
(Instant AP)(config)# wlan ssid-profile dot11r-profile
(Instant AP)(SSID Profile "dot11r-profile")# dot11r
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Radio Resource Management (802.11k)

The 802.11k protocol provides mechanisms for APs and clients to dynamically measure the available radio resources and enables stations to query and manage their radio resources. In an 802.11k enabled network, APs and clients can share radio and link measurement information, neighbor reports, and beacon reports with each other. This allows the WLAN network infrastructural elements and clients to assess resources and make optimal mobility decisions to ensure Quality of Service (QoS) and seamless continuity.

Instant supports the following radio resource management information elements with 802.11k support enabled:

- *Power Constraint IE*–The power constraint element contains the information necessary to allow a client to determine the local maximum transmit power in the current channel.
- *AP Channel Report IE*–The AP channel report element contains a list of channels in a regulatory class where a client is likely to find an AP, including the AP transmitting the AP channel report.
- *RRM Enabled Capabilities IE*–The RRM Enabled Capabilities element signals support for radio measurements in a device. The clients use this IE to specify their radio measurement capabilities.
- *BSS Load Element*: The BSS Load element contains information on the density of clients and traffic levels in the QBSS.
- *Transmit Power Control (TPC) Report IE*: The TPC IE contains transmit power and link margin information.
- *Quiet IE*: The Quiet IE defines an interval during which no transmission occurs in the current channel. This interval may be used to assist in making channel measurements without interference from other stations in the BSS.

- *Extended Capabilities IE* - The extended capabilities IE carries information about the capabilities of an IEEE 802.11 station.

Beacon Report Requests and Probe Responses

The beacon request frame is sent by an AP to request a client to report the list of beacons heard by the client on all channels.

- The beacon request is sent using the radio measurement request action frame.
- It is sent only to those clients that have the capability to generate beacon reports. The clients indicate their capabilities through the *RRM enabled capabilities IE* sent in the association request frames.
- By default, the beacon request frames are sent at a periodicity of 60 seconds.

Configuring a WLAN SSID for 802.11k Support

You can enable 802.11k support on a WLAN SSID by using the Instant UI or CLI.

In the Instant UI

1. Navigate to the WLAN wizard (click **Network**>**New** or **Network**> Select the WLAN SSID>**edit**).
2. Click the **Security** tab.
3. Under **Fast Roaming**, Select the **802.11k** checkbox.
4. Click **Next** and then click **Finish**.

To allow the AP and clients to exchange neighbor reports, ensure that the Client match is enabled through **RF > ARM > Client match > Enabled** in the UI or by executing the **client-match** command in the **arm** configuration sub-mode.

In the CLI

To enable 802.11k profile:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# dot11k
(Instant AP)(config)# end
(Instant AP)# commit apply
```

To view the beacon report details:

```
show ap dot11k-beacon-report <mac>
```

To view the neighbor details:

```
show ap dot11k-nbrs
```

Example

```
(Instant AP)(config)# wlan ssid-profile dot11k-profile
(Instant AP)(SSID Profile "dot11k-profile")# dot11k
(Instant AP)(config)# end
(Instant AP)# commit apply
```

BSS Transition Management (802.11v)

The 802.11v standard provides Wireless Network Management enhancements to the IEEE 802.11 MAC and PHY. It extends radio measurements to define mechanisms for wireless network management of stations including BSS transition management.

W-IAPs support the generation of the BSS transition management request frames to the 802.11k clients when a suitable AP is identified for a client through client match.

Configuring a WLAN SSID for 802.11v Support

You can enable 802.11v support on a WLAN SSID by using the Instant UI or CLI.

In the Instant UI

1. Navigate to the WLAN wizard (click **Network**>**New** or **Network**> Select the WLAN SSID>**edit**).
2. Click the **Security** tab.
3. Under **Fast Roaming**, Select the **802.11v** checkbox.
4. Click **Next** and then click **Finish**.

In the CLI

To enable 802.11v profile:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# dot11v
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Example

```
(Instant AP)(config)# wlan ssid-profile dot11v-profile
(Instant AP)(SSID Profile "dot11v-profile")# dot11v
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Editing Status of a WLAN SSID Profile

You can enable or disable an SSID profile in the Instant UI or CLI.

In the Instant UI

To modify the status of a WLAN SSID profile:

1. In the **Networks** tab, select the network that you want to edit. The **edit** link is displayed.
2. Click the **edit** link. The **Edit network** window is displayed.
3. Select or clear the **Disable SSID** checkbox to disable or enable the SSID. The SSID is enabled by default.
4. Click **Next** or the tab name to move to the next tab.
5. Click **Finish** to save the modifications.

In the CLI

To disable an SSID

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# disable
(Instant AP)(SSID Profile <name>)# end
(Instant AP)# commit apply
```

To enable an SSID:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# enable
(Instant AP)(SSID Profile <name>)# end
(Instant AP)# commit apply
```

Editing a WLAN SSID Profile

To edit a WLAN SSID profile:

1. In the **Networks** tab, select the network that you want to edit. The **edit** link is displayed.

2. Click the **edit** link. The **Edit network** window is displayed.
3. Modify the required settings. Click **Next** to move to the next tab.
4. Click **Finish** to save the modifications.

Deleting a WLAN SSID Profile

To delete a WLAN SSID profile:

1. In the **Networks** tab, click the network that you want to delete. A **x** link is displayed against the network to be deleted.
2. Click **x**. A delete confirmation window is displayed.
3. Click **Delete Now**.

This chapter describes the following procedures:

- Configuring a Wired Profile on page 112
- Assigning a Profile to Ethernet Ports on page 117
- Editing a Wired Profile on page 117
- Deleting a Wired Profile on page 118
- Link Aggregation Control Protocol for W-IAP220 Series on page 118
- Understanding Hierarchical Deployment on page 119

Configuring a Wired Profile

The Ethernet ports allow third-party devices such as VoIP phones or printers (which support only wired connections) to connect to the wireless network. You can also configure an Access Control List (ACL) for additional security on the Ethernet downlink.

The wired profile configuration for employee network involves the following procedures:

1. Configuring Wired Settings on page 112
2. Configuring VLAN for a Wired Profile on page 114
3. Configuring Security Settings for a Wired Profile on page 115
4. Configuring Access Rules for a Wired Profile on page 116

For information on creating a wired profile for guest network, see Captive Portal for Guest Access

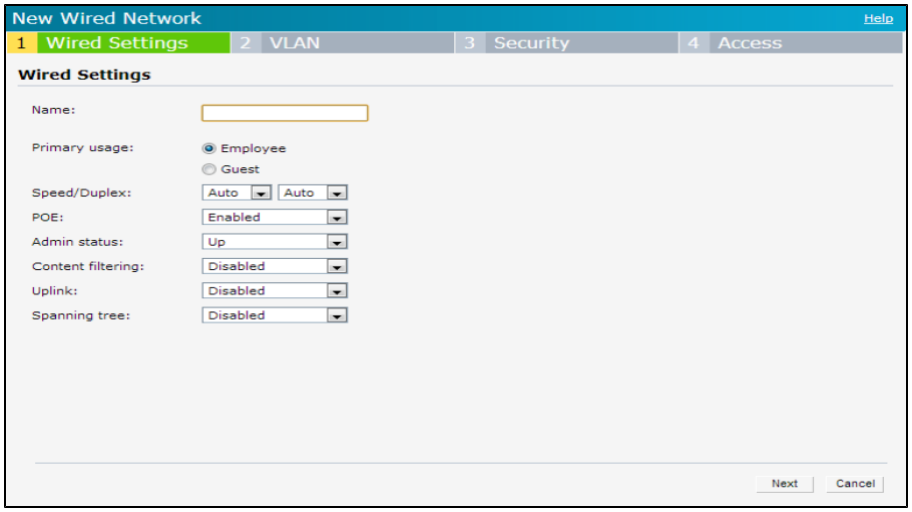
Configuring Wired Settings

You can configure wired settings for a wired profile by using the Instant UI or CLI.

In the Instant UI

1. Click the **Wired** link under **More** at the top right corner of the Instant main window. The **Wired** window is displayed.
2. Click **New** under **Wired Networks**. The **New Wired Network** window is displayed. The following figure shows the contents of the **Wired Settings** tab:

Figure 38 *New Wired Network Window: Wired Settings Window*



3. Click the **Wired Settings** tab and enter the following information:
   a. **Name**– Specify a name for the profile.
   b. **Primary Usage** – Select **Employee** or **Guest**.
   c. **Speed/Duplex** – Ensure that appropriate values are selected for **Speed/Duplex**. Contact your network administrator if you need to assign speed and duplex parameters.
   d. **POE** – Set **POE** to **Enabled** to enable Power over Ethernet.

NOTE

The E2 port on W-IAP3WNP supports Power Sourcing Equipment (PSE) to supply power to any compliant 802.3af powered (class 0-4) device. W-IAP155P supports PSE for 802.3af powered device (class 0-4) on one port (E1 or E2), or 802.3at powered DC IN (Power Socket) on two ports (E1 and E2).

   e. **Admin Status** – Ensure that an appropriate value is selected. The **Admin Status** indicates if the port is up or down.
   f. **Content Filtering**– To ensure that all DNS requests to non-corporate domains on this wired network are sent to OpenDNS, select **Enabled** for **Content Filtering**.
   g. **Uplink** – Select **Enabled** to configure uplink on this wired profile. If **Uplink** is set to **Enabled** and this network profile is assigned to a specific port, the port will be enabled as Uplink port. For more information on assigning a wired network profile to a port, see Assigning a Profile to Ethernet Ports on page 117.
   h. **Spanning Tree**–Select the **Spanning Tree** checkbox to enable Spanning Tree Protocol (STP) on the wired profile. STP ensures that there are no loops in any bridged Ethernet network and operates on all downlink ports, regardless of forwarding mode. STP will not operate on the uplink port and is supported only on W-IAPs with three or more ports. By default Spanning Tree is disabled on wired profiles.
4. Click **Next**. The VLAN tab details are displayed.
5. Configure VLAN for the wired profile. For more information, see Configuring VLAN for a Wired Profile on page 114.

In the CLI

To configure wired settings for:

```
(Instant AP)(config)# wired-port-profile <name>
(Instant AP)(wired ap profile <name>)# type {<employee> |<guest>}
(Instant AP)(wired ap profile <name>)# speed {10 |100 |1000 |auto}
(Instant AP)(wired ap profile <name>)# duplex {half|full|auto}
(Instant AP)(wired ap profile <name>)# no shutdown
(Instant AP)(wired ap profile <name>)# poe
```

```
(Instant AP)(wired ap profile <name>)# uplink-enable
(Instant AP)(wired ap profile <name>)# content-filtering
(Instant AP)(wired ap profile <name>)# spanning-tree
(Instant AP)(wired ap profile <name>)# end
(Instant AP)# commit apply
```

Configuring VLAN for a Wired Profile

If you are creating a new wired profile, complete the Wired Settings procedure before configuring VLAN. For more information, see Configuring Wired Settings on page 112.

You can configure VLAN using the Instant UI or CLI.

In the Instant UI

To configure VLAN:

1. In the **VLAN** tab, enter the following information.
   a. **Mode** – You can specify any of the following modes:
      - **Access** – Select this mode to allow the port to carry a single VLAN specified as the native VLAN.
      - **Trunk** – Select this mode to allow the port to carry packets for multiple VLANs specified as allowed VLANs.
   b. Specify any of the following values for **Client IP Assignment**:
      - **Virtual Controller Assigned**: Select this option to allow the Virtual Controller to assign IP addresses to the wired clients. When the Virtual Controller assignment is used, the source IP address is translated for all client traffic that goes through this interface. The Virtual Controller can also assign a guest VLAN to a wired client.
      - **Network Assigned**: Select this option to allow the clients to receive an IP address from the network to which the Virtual Controller is connected. On selecting this option, the **New** button to create a VLAN is displayed. Create a new VLAN if required.
   c. If the **Trunk** mode is selected:
      - Specify the **Allowed VLAN**, enter a list of comma separated digits or ranges 1,2,5 or 1-4, or all. The Allowed VLAN refers to the VLANs carried by the port in Access mode.
      - If the **Client IP Assignment** is set to **Network Assigned**, specify a value for **Native VLAN**. A VLAN that does not have a VLAN ID tag in the frames is referred to as Native VLAN. You can specify a value within the range of 1-4093.
   d. If the **Access** mode is selected:
      - If the **Client IP Assignment** is set to **Virtual Controller Assigned**, proceed to step 2.
      - If the **Client IP Assignment** is set to **Network Assigned**, specify a value for **Access VLAN** to indicate the VLAN carried by the port in the **Access** mode.
2. Click **Next**. The **Security** tab details are displayed.
3. Configure security settings for the wired profile. For more information, see Configuring Security Settings for a Wired Profile on page 115.

In the CLI

To configure VLAN settings for a wired profile:

```
(Instant AP)(config)# wired-port-profile <name>
(Instant AP)(wired ap profile <name>)# switchport-mode {trunk|access}
(Instant AP)(wired ap profile <name>)# allowed-vlan <vlan>
(Instant AP)(wired ap profile <name>)# native-vlan {<guest|1…4095>}
(Instant AP)(wired ap profile <name>)# end
```

```
(Instant AP)# commit apply
```

To configure a new VLAN assignment rule:

```
(Instant AP)(config)# wired-port-profile <name>
(Instant AP)(wired ap profile <name>)# set-vlan <attribute>{equals| not-equals| starts-with|
ends-with| contains| matches-regular-expression} <operator> <VLAN-ID>| value-of}
(Instant AP)(wired ap profile <name>)# end
(Instant AP)# commit apply
```

Configuring Security Settings for a Wired Profile

If you are creating a new wired profile, complete the Wired Settings and VLAN procedures before specifying security settings. For more information, see Configuring Wired Settings on page 112 and Configuring VLAN Settings for a WLAN SSID Profile on page 97.

Configuring Security Settings for a Wired Employee Network

You can configure security parameters for an employee network by using the Instant UI or CLI.

In the Instant UI

To configure security parameters for an employee network:

1. Configure the following parameters in the **Security** tab.
   - **MAC authentication** – To enable MAC authentication, select **Enabled**. The MAC authentication is disabled by default.
   - **802.1X authentication** – To enable 802.1X authentication, select **Enabled**.
   - **MAC authentication fail-thru** – To enable authentication fail-thru, select **Enabled**. When this feature is enabled, 802.1X authentication is attempted when MAC authentication fails. The **MAC authentication fail-thru** checkbox is displayed only when both **MAC authentication** and **802.1X authentication** are **Enabled**.
   - Select any of the following options for **Authentication server 1**:
     - **New** – On selecting this option, an external RADIUS server must be configured to authenticate the users. For information on configuring an external server, see Configuring an External Server for Authentication on page 157.Authentication and User Management on page 140
     - **Internal server**– If an internal server is selected, add the clients that are required to authenticate with the internal RADIUS server. Click the **Users** link to add the users. For information on adding a user, see Managing W-IAP Users on page 140.
   - **Reauth interval** – Specify the interval at which all associated and authenticated clients must be reauthenticated.
   - **Load balancing**– Set this to **Enabled** if you are using two RADIUS authentication servers, so that the load across the two RADIUS servers is balanced. For more information on the dynamic load balancing mechanism, see Dynamic Load Balancing between Two Authentication Servers on page 154.
2. Click **Next**. The **Access** tab details are displayed.

In the CLI

To configure security settings for an employee network:

```
(Instant AP)(config)# wired-port-profile <name>
(Instant AP)(wired ap profile <name>)# mac-authentication
(Instant AP)(wired ap profile <name>)# l2-auth-failthrough
(Instant AP)(wired ap profile <name>)# auth-server <name>
(Instant AP)(wired ap profile <name>)# server-load-balancing
(Instant AP)(wired ap profile <name>)# radius-reauth-interval <Minutes>
(Instant AP)(wired ap profile <name>)# end
(Instant AP)# commit apply
```

Configuring Access Rules for a Wired Profile

The Ethernet ports allow third-party devices such as VoIP phones or printers (that support only wired connections) to connect to the wireless network. You can also configure an Access Control List (ACL) for additional security on the Ethernet downlink.

NOTE

If you are creating a new wired profile, complete the Wired Settings and configure VLAN and security parameters, before defining access rules. For more information, see Configuring Wired Settings on page 112, Configuring VLAN for a Wired Profile on page 114, and Configuring Security Settings for a Wired Profile on page 115.

You can configure access rules by using the Instant UI or CLI.

In the Instant UI

To configure access rules:

1. In the **Access** tab, configure the following access rule parameters.
   a. Select any of the following types of access control:
      - **Role-based**– Allows the users to obtain access based on the roles assigned to them.
      - **Unrestricted**– Allows the users to obtain unrestricted access on the port.
      - **Network-based**– Allows the users to be authenticated based on access rules specified for a network.
   b. If the **Role-based** access control is selected, perform the following steps:
      - Under **Roles**, select an existing role for which you want to apply the access rules, or click **New** and add the required role. The list of roles defined for all networks is displayed under **Roles**.

NOTE

The default role with the same name as the network, is automatically defined for each network. The default roles cannot be modified or deleted.

      - Select the access rule associated with a specific role and modify if required. To add a new access rule, click **New** in the **Access Rules** window. You can configure up to 64 access rules. For more information on configuring access rules, see Configuring Access Rules for Network Services on page 177.
      - Configure rules to assign roles for an authenticated client. You can also configure rules to derive VLANs for the wired network profile. For more information on role assignment rules and VLAN derivation rules, see Configuring Derivation Rules on page 192 and Configuring VLAN Derivation Rules on page 196.
      - Select the **Assign pre-authentication role** checkbox to add a pre-authentication role that allows some access to the users before the client authentication.
      - Select the **Enforce Machine Authentication** checkbox, to configure access rights to clients based on whether the client device supports machine authentication. Select the **Machine auth only** and **User auth** only rules. Machine Authentication is only supported on Windows devices and devices such as iPads.

NOTE

If **Enforce Machine Authentication** is enabled, both the device and the user must be authenticated for the role assignment rule to apply.

2. Click **Finish**.

In the CLI

To configure access rules for a wired profile:

```
(Instant AP)(config)# wired-port-profile <name>
(Instant AP)(wired ap profile <name>)# access-rule-name <name>
(Instant AP)(wired ap profile <name>)# end
(Instant AP)# commit apply
```

To configure role assignment rules:

```
(Instant AP)(config)# wired-port-profile <name>
(Instant AP)(wired ap profile <name>)# set-role <attribute>{{equals| not-equal| starts-with|
ends-with| contains| matches-regular-expression}<operator> <role>| value-of}
(Instant AP)(wired ap profile <name>)# end
(Instant AP)# commit apply
```

To configure a pre-authentication role:

```
(Instant AP)(config)# wired-port-profile <name>
(Instant AP)(wired ap profile <name>)# set-role-pre-auth <pre-authentication-role>
(Instant AP)(wired ap profile <name>)# end
(Instant AP)# commit apply
```

To configure machine and user authentication roles:

```
(Instant AP)(config)# wired-port-profile <name>
(Instant AP)(wired ap profile <name>)# set-role-machine-auth <machine_only> <user-only>
(Instant AP)(wired ap profile <name>)# end
(Instant AP)# commit apply
```

To configure unrestricted access:

```
(Instant AP)(config)# wired-port-profile <name>
(Instant AP)(wired ap profile <name>)# set-role-unrestricted
(Instant AP)(wired ap profile <name>)# end
(Instant AP)# commit apply
```

Assigning a Profile to Ethernet Ports

You can assign profiles to Ethernet ports using the Instant UI or CLI.

In the Instant UI

To assign profiles to Ethernet ports:

1. Click the **Wired** link under **More** at the top right corner of the Instant main window. The **Wired** window is displayed.
2. To assign an Ethernet downlink profile to Ethernet 0 port:
   a. Ensure that the wired bridging on the port is enabled. For more information, see Configuring Wired Bridging on Ethernet 0 for Mesh Point on page 304.
   b. Select and assign a profile from the **0/0** drop down list.
   c. To assign a wired profile to Ethernet 0/1 port, select the profile from the **0/1** drop down list.
   d. If the W-IAP supports E2, E3 and E4 ports, assign profiles to other Ethernet ports by selecting a profile from the **0/2**, **0/3**, and **0/4** drop-down list.

In the CLI

To assign profiles to Ethernet ports:

```
(Instant AP)(config)# enet0-port-profile <name>
(Instant AP)(config)# enet1-port-profile <name>
(Instant AP)(config)# enet2-port-profile <name>
(Instant AP)(config)# enet3-port-profile <name>
(Instant AP)(config)# enet4-port-profile <name>
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Editing a Wired Profile

To edit a wired profile:

1. Click the **Wired** link under **More** at the top right corner of the Instant main window. The **Wired** window is displayed.
2. In the **Wired** window, select the wired profile to modify.
3. Click **Edit**. The **Edit Wired Network** window is displayed.
4. Modify the required settings.
5. Click **Finish** to save the modifications.

Deleting a Wired Profile

To delete a wired profile:

1. Click the **Wired** link under **More** at the top right corner of the Instant main window. The **Wired** window is displayed.
2. In the **Wired** window, select the wired profile to delete.
3. Click **Delete**. The wired profile is deleted.

Link Aggregation Control Protocol for W-IAP220 Series

W-IAP220 Series supports the IEEE 802.11ac standard for high-performance WLAN. To support maximum traffic, port aggregation is required as it increases throughput and enhances reliability. To support port aggregation, Instant supports Link Aggregation Control Protocol (LACP) based on the IEEE 802.3ad standard. 802.3ad standard for Ethernet aggregation uses LACP as a method to manage link configuration and balance traffic among aggregated ports.

LACP provides a standardized means for exchanging information with partner systems to form a dynamic link aggregation group. The LACP feature is automatically enabled during W-IAP boots and it dynamically detects the AP if connected to a partner system with LACP capability, by checking if there is any LACP Protocol Data Unit (PDU) received on either eth0 or eth1 port.

If the switch in the cluster has the LACP capability, you can combine eth0 and eth1 interfaces into the link aggregation group to form a single logical interface (port-channel). Port-channels can be used to provide additional bandwidth or link redundancy between two devices. W-IAP220 Series supports link aggregation using either standard port-channel (configuration based) or Link Aggregation Control Protocol (protocol signaling based). W-IAP220 Series can optionally be deployed with LACP configuration to benefit from the higher (greater than 1 Gbps) aggregate throughput capabilities of the two radios.

The LACP feature is supported only on W-IAP220 Series.

There is no configuration required on the AP for enabling LACP support. However, you can view the status of LACP on W-IAPs by using the following command:

```
(Instant AP)# show lacp status
AP LACP Status
--------------
Link Status LACP Rate Num Ports Actor Key Partner Key Partner MAC
----------- --------- --------- --------- ----------- -----------
Up slow 2 17 1 70:81:05:11:3e:80
Slave Interface Status
----------------------
Slave I/f Name Permanent MAC Addr Link Status Member of LAG Link Fail Count
-------------- ------------------ ----------- ------------- ---------------
eth0 6c:f3:7f:c6:76:6e Up Yes 0
eth1 6c:f3:7f:c6:76:6f Up Yes 0
Traffic Sent on Enet Ports
```

```
-------------------------
Radio Num Enet 0 Tx Count Enet 1 Tx Count
--------- -------------- --------------
0 0 0
1 0 0
non-wifi 2 17
```

Understanding Hierarchical Deployment

A W-IAP130 Series or W-IAP3WN (with more than one wired port) can be connected to the downlink wired port of another W-IAP (ethX). A W-IAP with a single Ethernet port (like W-IAP90 or W-IAP100 series devices) can be provisioned to use Ethernet bridging, so that Ethernet 0 port is converted to a downlink wired port.

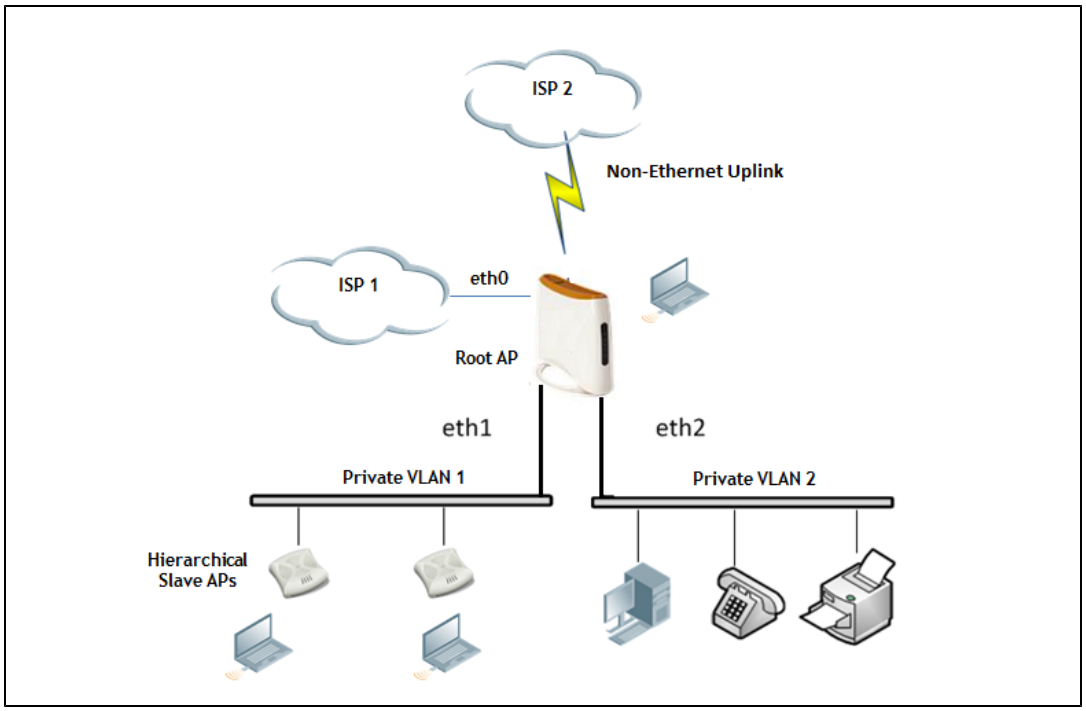
You can also form a W-IAP network by connecting the downlink port of an AP to other APs. Only one AP in the network uses its downlink port to connect to the other APs. This AP (called the root AP) acts as the wired device for the network, provides DHCP service and an L3 connection to the ISP uplink with NAT. The root AP is always the master of the Instant network. In a single Ethernet port platform deployment, the root AP must be configured to use the 3G uplink.

A typical hierarchical deployment consists of the following:

- A direct wired ISP connection or a wireless uplink.
- One or more DHCP pools for private VLANs.
- One downlink port configured on a private VLAN without authentication for connecting to slave APs. Ensure that the downlink port configured in a private VLAN is not used for any wired client connection. Other downlink ports can be used for connecting to the wired clients.

The following figure illustrates a hierarchical deployment scenario:

Figure 39 *Hierarchical Deployment*



This chapter provides the following information:

- Understanding Captive Portal on page 120
- Configuring a WLAN SSID for Guest Access on page 121
- Configuring Wired Profile for Guest Access on page 125
- Configuring Internal Captive Portal for Guest Network on page 126
- Configuring External Captive Portal for a Guest Network on page 129
- Configuring External Captive Portal Authentication Using ClearPass Guest on page 132
- Configuring Guest Logon Role and Access Rules for Guest Users on page 133
- Configuring Captive Portal Roles for an SSID on page 135
- Configuring Walled Garden Access on page 138
- Disabling Captive Portal Authentication on page 138

Understanding Captive Portal

Instant supports the captive portal authentication method, where a Web page is presented to the guest users when they try to access the Internet whether in hotels, conference centers or Wi-Fi hotspots. The Web page also prompts the guest users to authenticate or accept the usage policy and terms. captive portals are used at many Wi-Fi hotspots and can be used to control wired access as well.

The Instant captive portal solution consists of the following:

- The captive portal Web login page hosted by an internal or external server.
- The RADIUS authentication or user authentication against W-IAP's internal database.
- The SSID broadcast by the W-IAP.

With Instant, the administrators can create a wired or WLAN guest network based on captive portal authentication for guests, visitors, contractors, and any non-employee users who can use the enterprise Wi-Fi network. The administrators can also create guest accounts and customize the captive portal page with organization-specific logo, terms, and usage policy. With captive portal authentication and guest profiles, the devices associating with the guest SSID are assigned an initial role and are assigned IP addresses. When a guest user tries to access a URL through HTTP or HTTPS, the captive portal web page prompting the user to authenticate with a user name and password is displayed.

Types of Captive Portal

Instant supports the following types of captive portal authentication:

- **Internal captive portal** – For Internal captive portal authentication, an internal server is used for hosting the captive portal service. It supports the following types of authentication:
  - **Internal Authenticated**– When **Internal Authenticated** is enabled, a guest user must authenticate in the captive portal page to access the Internet. The guest users who are required to authenticate must already be added to the user database.
  - **Internal Acknowledged**– When **Internal Acknowledged** is enabled, a guest user must accept the terms and conditions to access the Internet.

- **External captive portal**– For external captive portal authentication, an external portal on the cloud or on a server outside the enterprise network is used.

Walled Garden

The administrators can also control the resources that the guest users can access and the amount of bandwidth or air time they can use at any given time. When an external captive portal is used, the administrators can configure a walled garden, which determines access to the URLs requested by the guest users. For example, a hotel environment where the unauthenticated users are allowed to navigate to a designated login page (for example, a hotel website) and all its contents. The users who do not sign up for the Internet service can view only the "allowed" websites (typically hotel property websites).

The administrators can allow or block access to specific URLs by creating a whitelist and blacklist. When the users attempt to navigate to other websites, which are not in the whitelist of the walled garden profile, the users are redirected to the login page. If the requested URL is on the blacklist, it is blocked. If it appears on neither list, the request is redirected to the external captive portal.

Configuring a WLAN SSID for Guest Access

You create an SSID for guest access by using the Instant UI or CLI:

In the Instant UI

1. In the **Networks** tab of the Instant main window, click the **New** link. The **New WLAN** window is displayed.
2. Enter a name that uniquely identifies a wireless network in the **Name (SSID)** text box.
3. Based on the type of network profile, specify the **Primary usage** as **Guest**.
4. Click the **Show advanced options** link. The advanced options for configuration are displayed.
5. Enter the required values for the following configuration parameters:

Table 22: *WLAS SSID Configuration Parameters for Guest Network*

Parameters	Description
Broadcast/Multicast	Select any of the following values under **Broadcast filtering**: • **All**–When set to **All**, the W-IAP drops all broadcast and multicast frames except DHCP and ARP. • **ARP**–When set to **ARP**, the W-IAP converts ARP requests to unicast and send frames directly to the associated client. • **Disabled**– When set to **Disabled**, all broadcast and multicast traffic is forwarded.
DTIM interval	The **DTIM interval** indicates the delivery traffic indication message (DTIM) period in beacons, which can be configured for every WLAN SSID profile. The DTIM interval determines how often the W-IAP should deliver the buffered broadcast and multicast frames to associated clients in the powersave mode. The default value is 1, which means the client checks for buffered data on the W-IAP at every beacon. You can also configure a higher DTIM value for power saving.
Multicast transmission optimization	Select **Enabled** if you want the W-IAP to select the optimal rate for sending broadcast and multicast frames based on the lowest of unicast rates across all associated clients. When this option is enabled, multicast traffic can be sent at up to 24 Mbps. The default rate for sending frames for 2.4 GHz is 1 Mbps and 5.0 GHz is 6 Mbps. This option is disabled by default.

Parameters	Description
Dynamic multicast optimization	Select **Enabled** to allow W-IAP to convert multicast streams into unicast streams over the wireless link. Enabling Dynamic Multicast Optimization (DMO) enhances the quality and reliability of streaming video, while preserving the bandwidth available to the non-video clients.
DMO channel utilization threshold	Specify a value to set a threshold for DMO channel utilization. With DMO, the W-IAP converts multicast streams into unicast streams as long as the channel utilization does not exceed this threshold. The default value is 90% and the maximum threshold value is 100%. When the threshold is reached or exceeds the maximum value, the W-IAP sends multicast traffic over the wireless link. **NOTE:** When you enable DMO on multicast SSID profiles, ensure that the DMO feature is enabled on all SSIDs configured in the same VLAN.
Transmit Rates	Specify the following parameters: • **2.4 GHz**–If the 2.4 GHz band is configured on the W-IAP, specify the minimum and maximum transmission rate. The default value for minimum transmission rate is 1 Mbps and maximum transmission rate is 54 Mbps. • **5 GHz**–If the 5 GHz band is configured on the W-IAP, specify the minimum and maximum transmission rate. The default value for minimum transmission rate is 6 Mbps and maximum transmission rate is 54 Mbps.
Zone	Specify the zone for the SSID. When the zone is defined in SSID profile and if the same zone is defined on a W-IAP, the SSID is created on that W-IAP. For more information on configuring zone details on an IAP, see Configuring Zone Settings on a W-IAP on page 84. The following constraints apply to the zone configuration: • A W-IAP can belong to only one zone and only one zone can be configured on an SSID. • If an SSID belongs to a zone, all W-IAPs in this zone can broadcast this SSID. If no W-IAP belongs to the zone configured on the SSID, the SSID is not broadcast. • If an SSID does not belong to any zone, all W-IAPs can broadcast this SSID.
Bandwidth Limits	Select any of the following checkboxes to specify the bandwidth limit: • **Airtime**–Select this checkbox to specify an aggregate amount of airtime that all clients in this network can use for sending and receiving data. Specify the airtime percentage. • **Each user**– Select this checkbox to specify a throughput for any single user in this network. Specify the throughput value in Kbps. • **Each radio**– Select this checkbox to specify an aggregate amount of throughput that each radio is allowed to provide for the connected clients.
Wi-Fi Multimedia (WMM) traffic management	Configure the following options for WMM traffic management. WMM supports voice, video, best effort, and background access categories. To allocate bandwidth for the following types of traffic, specify a percentage value under **Share**. To configure DSCP mapping, specify a value under **DSCP Mapping**. • **Background WMM**: For background traffic such as file downloads or print jobs. • **Best effort WMM** – For best effort traffic such as traffic from legacy devices or traffic from applications or devices that do not support QoS. • **Video WMM** – For video traffic generated from video streaming. • **Voice WMM**– For voice traffic generated from the incoming and outgoing voice communication. For more information on WMM traffic and DSCP mapping, see Wi-Fi Multimedia Traffic Management on page 251
Content filtering	Set to **Enabled** to route all DNS requests for the non-corporate domains to OpenDNS on this network.

Parameters	Description
Band	Select a value to specify the band at which the network transmits radio signals. You can set the band to **2.4 GHz**, **5 GHz**, or **All**. The **All** option is selected by default.
Inactivity timeout	Specify a timeout interval. If a client session is inactive for the specified duration, the session expires and the users are required to log in again. The minimum value is set to 60 seconds and the default value is 1000 seconds.
Hide SSID	Select the checkbox if you do not want the SSID (network name) to be visible to users
Disable SSID	Select to the checkbox to disable the SSID. On selecting this checkbox, the SSID is disabled, but not removed from the network. By default, all SSIDs are enabled.
Can be used without Uplink	Select the checkbox if you do not want the SSID users to use uplink.
Max clients threshold	Specify the maximum number of clients that can be configured for each BSSID on a WLAN in the text box. You can specify a value within the range of 0 to 255. The default value is 64.
Local probe request threshold	Specify a threshold value in the **Local probe request threshold** text box to limit the number of incoming probe requests. When a client sends a broadcast probe request frame to search for all available SSIDs, this option controls system response for this network profile and ignores probe requests if required. You can specify a Received signal strength indication (RSSI) value within range of 0 to 100 dB.

6. Click **Next** to configure VLAN settings. The VLAN tab contents are displayed.
7. Select any for the following options for **Client IP assignment**:
   - **Virtual Controller assigned**–On selecting this option, the client obtains the IP address from the Virtual Controller.
   - **Network assigned**–On selecting this option, the IP address is obtained from the network.
8. Based on the type client IP assignment mode selected, you can configure the VLAN assignment for clients as described in the following table:

Table 23: *IP and VLAN Assignment for WLAN SSID Clients*

Client IP Assignment	Client VLAN Assignment
Virtual Controller assigned	If the **Virtual Controller assigned** is selected for client IP assignment, the Virtual Controller creates a private subnet and VLAN on the W-IAP for the wireless clients. The network address translation for all client traffic that goes out of this interface is carried out at the source. This setup eliminates the need for complex VLAN and IP address management for a multi-site wireless network. On selecting this option, the following client VLAN assignment options are displayed: • **Default**: When selected, the default VLAN as determined by the Virtual Controller is assigned for clients. • **Custom**: When selected, you can specify a custom VLAN assignment option. You can select an existing DHCP scope for client IP and VLAN assignment or you can create a new DHCP scope by selecting **New**. For more information on DHCP scopes, see Configuring DHCP Scopes on page 201.

Network assigned	If the **Network assigned** is selected, you can specify any of the following options for the **Client VLAN assignment**.
	• **Default**– On selecting this option, the client obtains the IP address in the same subnet as the W-IAPs. By default, the client VLAN is assigned to the native VLAN on the wired network.
	• **Static**– On selecting this option, you need to specify a single VLAN, a comma separated list of VLANS, or a range of VLANs for all clients on this network. Select this option for configuring VLAN pooling.
	• **Dynamic**– On selecting this option, you can assign the VLANs dynamically from a Dynamic Host Configuration Protocol (DHCP) server. To create VLAN assignment rules, click **New** to assign the user to a VLAN. In the **New VLAN Assignment Rule** window, enter the following information:
	
	  ◦ **Attribute**– Select an attribute returned by the RADIUS server during authentication.
	  ◦ **Operator**– Select an operator for matching the string.
	  ◦ **String**– Enter the string to match
	  ◦ **VLAN**– Enter the VLAN to be assigned.

9. Click **Next** to configure internal or external captive portal authentication, roles and access rules for the guest users.

In the CLI

To configure WLAN settings for an SSID profile:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# essid <ESSID-name>
(Instant AP)(SSID Profile <name>)# type <Guest>
(Instant AP)(SSID Profile <name>)# broadcast-filter <type>
(Instant AP)(SSID Profile <name># dtim-period <number-of-beacons>
(Instant AP)(SSID Profile <name>)# multicast-rate-optimization
(Instant AP)(SSID Profile <name>)# dynamic-multicast-optimization
(Instant AP)(SSID Profile <name>)# dmo-channel-utilization-threshold
(Instant AP)(SSID Profile <name>)# a-max-tx-rate <rate>
(Instant AP)(SSID Profile <name>)# a-min-tx-rate <rate>
(Instant AP)(SSID Profile <name>)# g-max-tx-rate <rate>
(Instant AP)(SSID Profile <name>)# g-min-tx-rate <rate>
(Instant AP)(SSID Profile <name>)# zone <zone>
(Instant AP)(SSID Profile <name>)# bandwidth-limit <limit>
(Instant AP)(SSID Profile <name>)# per-user-bandwidth-limit <limit>
(Instant AP)(SSID Profile <name>)# air-time-limit <limit>
(Instant AP)(SSID Profile <name>)# wmm-background-share <percentage-of-traffic_share>
(Instant AP)(SSID Profile <name>)# wmm-best-effort-share<percentage-of-traffic-share>
(Instant AP)(SSID Profile <name>)# wmm-video-share <percentage-of-traffic_share>
(Instant AP)(SSID Profile <name>)# wmm-voice-share <percentage-of-traffic_share>
```

```
(Instant AP)(SSID Profile <name>)# rf-band {<2.4>|<5.0>|<all>}
(Instant AP)(SSID Profile <name>)# content-filtering
(Instant AP)(SSID Profile <name>)# hide-ssid
(Instant AP)(SSID Profile <name>)# inactivity-timeout <interval>
(Instant AP)(SSID Profile <name>)# work-without-uplink
(Instant AP)(SSID Profile <name>)# local-probe-req-thresh <threshold>
(Instant AP)(SSID Profile <name>)# max-clients-threshold <number-of-clients>
```

To manually assign VLANs for WLAN SSID users:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name># vlan <vlan-ID>
```

To enforce DHCP-based VLAN assignment:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name># enforce-dhcp
```

To create a new VLAN assignment rule:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# set-vlan <attribute>{equals|not-equals| starts-with| ends-
with| contains|matches-regular-expression} <operator> <VLAN-ID>| value-of}
```

Configuring Wired Profile for Guest Access

You can configure wired settings for a wired profile by using the Instant UI or CLI.

In the Instant UI

1. Click the **Wired** link under **More** at the top right corner of the Instant main window. The **Wired** window is displayed.
2. Click **New** under **Wired Networks**. The **New Wired Network** window is displayed.
3. Click the **Wired Settings** tab and enter the following information:
   a. **Name**– Specify a name for the profile.
   b. **Primary Usage** – Select **Employee** or **Guest**.
   c. **Speed/Duplex** – Ensure that appropriate values are selected for **Speed/Duplex**. Contact your network administrator if you need to assign speed and duplex parameters.
   d. **POE** – Set **POE** to **Enabled** to enable Power over Ethernet.
   e. **Admin Status** – Ensure that an appropriate value is selected. The **Admin Status** indicates if the port is up or down.
   f. **Content Filtering**– To ensure that all DNS requests to non-corporate domains on this wired network are sent to OpenDNS, select **Enabled** for **Content Filtering**.
   g. **Uplink** – Select **Enabled** to configure uplink on this wired profile. If **Uplink** is set to **Enabled** and this network profile is assigned to a specific port, the port will be enabled as Uplink port. For more information on assigning a wired network profile to a port, see Assigning a Profile to Ethernet Ports on page 117.
   h. **Spanning Tree**–Select the **Spanning Tree** checkbox to enable Spanning Tree Protocol (STP) on the wired profile. STP ensures that there are no loops in any bridged Ethernet network and operates on all downlink ports, regardless of forwarding mode. STP will not operate on the uplink port and is supported only on W-IAPs with three or more ports. By default Spanning Tree is disabled on wired profiles.
4. Click **Next**. The VLAN tab details are displayed.
5. Enter the following information.
   a. **Mode** – You can specify any of the following modes:
      - **Access** – Select this mode to allow the port to carry a single VLAN specified as the native VLAN.

- **Trunk** – Select this mode to allow the port to carry packets for multiple VLANs specified as allowed VLANs.

b. Specify any of the following values for **Client IP Assignment**:
   - **Virtual Controller Assigned**: Select this option to allow the Virtual Controller to assign IP addresses to the wired clients. When the Virtual Controller assignment is used, the source IP address is translated for all client traffic that goes through this interface. The Virtual Controller can also assign a guest VLAN to a wired client.
   - **Network Assigned**: Select this option to allow the clients to receive an IP address from the network to which the Virtual Controller is connected. On selecting this option, the **New** button to create a VLAN is displayed. Create a new VLAN if required.

c. If the **Trunk** mode is selected:
   - Specify the **Allowed VLAN**, enter a list of comma separated digits or ranges 1,2,5 or 1-4, or all. The Allowed VLAN refers to the VLANs carried by the port in Access mode.
   - If the **Client IP Assignment** is set to **Network Assigned**, specify a value for **Native VLAN**. A VLAN that does not have a VLAN ID tag in the frames is referred to as Native VLAN. You can specify a value within the range of 1-4093.

d. If the **Access** mode is selected:
   - If the **Client IP Assignment** is set to **Virtual Controller Assigned**, proceed to step 2.
   - If the **Client IP Assignment** is set to **Network Assigned**, specify a value for **Access VLAN** to indicate the VLAN carried by the port in the **Access** mode.

6. Click **Next** to configure internal or external captive portal authentication, roles and access rules for the guest users.

In the CLI

To configure wired settings for:

```
(Instant AP)(config)# wired-port-profile <name>
(Instant AP)(wired ap profile <name>)# type <guest>
(Instant AP)(wired ap profile <name>)# speed {10 |100 |1000 |auto}
(Instant AP)(wired ap profile <name>)# duplex {half|full|auto}
(Instant AP)(wired ap profile <name>)# no shutdown
(Instant AP)(wired ap profile <name>)# poe
(Instant AP)(wired ap profile <name>)# uplink-enable
(Instant AP)(wired ap profile <name>)# content-filtering
(Instant AP)(wired ap profile <name>)# spanning-tree
```

To configure VLAN settings for a wired profile:

```
(Instant AP)(config)# wired-port-profile <name>
(Instant AP)(wired ap profile <name>)# switchport-mode {trunk|access}
(Instant AP)(wired ap profile <name>)# allowed-vlan <vlan>
(Instant AP)(wired ap profile <name>)# native-vlan {<guest|1…4095>}
```

To configure a new VLAN assignment rule:

```
(Instant AP)(config)# wired-port-profile <name>
(Instant AP)(wired ap profile <name>)# set-vlan <attribute>{equals| not-equals| starts-with|
ends-with| contains| matches-regular-expression} <operator> <VLAN-ID>| value-of}
```

Configuring Internal Captive Portal for Guest Network

In the Internal Captive Portal type, an internal server is used for hosting the captive portal service. You can configure internal captive portal authentication when adding or editing a guest network created for wireless or wired profile through the Instant UI or CLI.

In the Instant UI

1. Navigate to the WLAN wizard or Wired window.
   - To configure internal captive portal authentication for a WLAN SSID, in the **Network** tab, click **New** to create a new network profile or **edit** to modify an existing profile.
   - To configure internal captive portal authentication for a wired profile, click **More**>**Wired**. In the **Wired** window, click **New** under **Wired Networks** to create a new network, or click **Edit** to select an existing profile.
2. Click the **Security** tab and assign values for the configuration parameters:

Table 24: *Internal Captive Portal Configuration Parameters*

Parameter	Description
Splash page type	Select any of the following from the drop-down list. • **Internal - Authenticated**–When **Internal Authenticated** is enabled, the guest users are required to authenticate in the captive portal page to access the Internet. The guest users who are required to authenticate must already be added to the user database. • **Internal - Acknowledged**– When **Internal Acknowledged** is enabled, the guest users are required to accept the terms and conditions to access the Internet.
MAC authentication	Select **Enabled** from the drop-down list to enable the MAC authentication.
WISPr (Applicable for WLAN SSIDs only.)	Select **Enabled** if you want to enable WISPr authentication. For more information on WISPr authentication, see Configuring WISPr Authentication on page 170. **NOTE:** The WISPr authentication is applicable only for Internal-Authenticated splash pages and is not applicable for wired profiles.
Auth server 1 **Auth server 2**	Select any one of the following: • A server from the list of servers if the server is already configured. • **Internal Server** to authenticate user credentials at run time. • Select **New** for configuring a new external RADIUS or LDAP server for authentication.
Load balancing	Select **Enabled** to enable load balancing if two authentication servers are used.
Reauth interval	Select a value to allow the APs to periodically reauthenticate all associated and authenticated clients.
Blacklisting (Applicable for WLAN SSIDs only.)	If you are configuring a wireless network profile, select **Enabled** to enable blacklisting of the clients with a specific number of authentication failures.
Accounting mode (Applicable for WLAN SSIDs only.)	Select an accounting mode from **Accounting mode** for posting accounting information at the specified **Accounting interval**. When the accounting mode is set to **Authentication**, the accounting starts only after client authentication is successful and stops when the client logs out of the network. If the accounting mode is set to **Association**, the accounting starts when the client associates to the network successfully and stops when the client is disconnected.

Parameter	Description
Disable if uplink type is	To exclude uplink, select an uplink type.
Encryption (Applicable for WLAN SSIDs only.)	Select **Enabled** to configure encryption parameters.
Splash Page Design	Under **Splash Page Visuals**, use the editor to specify text and colors for the initial page that will be displayed to the users connecting to the network. The initial page asks for user credentials or email, depending on the splash page type (Internal - Authenticated or Internal -Acknowledged) for which you are customizing the splash page design. Perform the following steps to customize the splash page design. • To change the color of the splash page, click the Splash page rectangle and select the required color from the **Background Color** palette. • To change the welcome text, click the first square box in the splash page, type the required text in the **Welcome** text box, and click **OK**. Ensure that the welcome text does not exceed 127 characters. • To change the policy text, click the second square in the splash page, type the required text in the **Policy** text box, and click **OK**. Ensure that the policy text does not exceed 255 characters. • To upload a custom logo, click **Upload your own custom logo Image**, browse the image file, and click **upload image**. Ensure that the image file size does not exceed 16 KB. • To redirect users to another URL, specify a URL in **Redirect URL**. • Click **Preview** to preview the Captive Portal page. **NOTE:** You can customize the captive portal page using double-byte characters. Traditional Chinese, Simplified Chinese, and Korean are a few languages that use double-byte characters. Click on the banner, term, or policy in the **Splash Page Visuals** to modify the text in the red box. These fields accept double-byte characters or a combination of English and double-byte characters.

3. Click **Next** to configure access rules.

In the CLI

To configure internal captive portal authentication:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# essid <ESSID-name>
(Instant AP)(SSID Profile <name>)# type <Guest>
(Instant AP)(SSID Profile <name>)# captive-portal <internal-authenticated> exclude-uplink
{3G|4G|Wifi|Ethernet}
(Instant AP)(SSID Profile <name>)# mac-authentication
(Instant AP)(SSID Profile <name>)# auth-server <server1>
(Instant AP)(SSID Profile <name>)# radius-reauth-interval <Minutes>
(Instant AP)(SSID Profile <name>)# end
(Instant AP)# commit apply
```

To configure internal captive portal for a wired profile:

```
(Instant AP) (config)# wired-port-profile <name>
(Instant AP) (wired ap profile <name>)# type <guest>
(Instant AP) (wired ap profile <name>)# captive-portal {<internal-authenticated>| <internal-
acknowledged>} exclude-uplink {3G|4G|Wifi|Ethernet}
(Instant AP) (wired ap profile <name>)# mac-authentication
(Instant AP) (wired ap profile <name>)# auth-server <server1>
(Instant AP) (wired ap profile <name>)# radius-reauth-interval <Minutes>
(Instant AP) (wired ap profile <name>)# end
(Instant AP)# commit apply
```

To customize internal captive portal splash page:

```
(Instant AP)(config)# wlan captive-portal
(Instant AP)(Captive Portal)# authenticated
(Instant AP)(Captive Portal)# background-color <color-indicator>
(Instant AP)(Captive Portal)# banner-color <color-indicator>
(Instant AP)(Captive Portal)# banner-text <text>
(Instant AP)(Captive Portal)# decoded-texts <text>
(Instant AP)(Captive Portal)# redirect-url <url>
(Instant AP)(Captive Portal)# terms-of-use <text>
(Instant AP)(Captive Portal)# use-policy <text>
(Instant AP)(Captive Portal)# end
(Instant AP)# commit apply
```

To upload a customized logo from a TFTP server to the W-IAP:

```
(Instant AP)# copy config tftp <ip-address> <filename> portal logo
```

Configuring External Captive Portal for a Guest Network

This section provides the following information:

- External Captive Portal Profiles on page 129
- Creating a Captive Portal Profile on page 129
- Configuring an SSID or Wired Profile to Use External Captive Portal Authentication on page 131

External Captive Portal Profiles

You can now configure external captive portal profiles and associate these profiles to a user role or SSID. You can create a set of captive portal profiles in the **Security>External Captive Portal** window and associate these profiles with an SSID or a wired profile. You can also create a new captive portal profile under the **Security** tab of the WLAN wizard or a Wired Network window. In the current release, you can configure up to eight external captive portal profiles.

When the captive portal profile is associated to an SSID, it is used before user authentication. If the profile is associated to a role, it is used only after the user authentication. When a captive portal profile is applied to an SSID or wired profile, the users connecting to the SSID or wired network are assigned a role with the captive portal rule. The guest user role allows only DNS and DHCP traffic between the client and network, and directs all HTTP or HTTPS requests to the captive portal unless explicitly permitted.

Creating a Captive Portal Profile

You can create a captive portal profile using the Instant UI or CLI.

In the Instant UI

1. Click **Security**>**External Captive Portal**.
2. Click **New**. The **New** pop-up window is displayed.
3. Specify values for the following parameters:

Table 25: *Captive Portal Profile Configuration Parameters*

Parameter	Description
Name	Enter a name for the profile.
Type	Select any one of the following types of authentication: • **Radius Authentication** - Select this option to enable user authentication against a RADIUS server. • **Authentication Text** - Select this option to specify an authentication text. The specified text will be returned by the external server after a successful user authentication.
IP or hostname	Enter the IP address or the hostname of the external splash page server.
URL	Enter the URL for the external captive portal server.
Port	Enter the number of the port to use for communicating with the external captive portal server.
Use https (Available only if RADIUS Authentication is selected)	Select **Enabled** to enforce clients to use HTTPS to communicate with the captive portal server.
Captive Portal failure	This field allows you to configure Internet access for the guest clients when the external captive portal server is not available. Select **Deny Internet** to prevent clients from using the network, or **Allow Internet** to allow the guest clients to access Internet when the external captive portal server is not available.
Automatic URL Whitelisting	Select **Enabled** or **Disabled** to enable or disable automatic whitelisting of URLs. On selecting the checkbox for the external captive portal authentication, the URLs that are allowed for the unauthenticated users to access are automatically whitelisted. The automatic URL whitelisting is disabled by default.
Auth Text (Available only if Authentication Text is selected)	If the External Authentication splash page is selected, specify the authentication text that must be returned by the external server after successful authentication.
Redirect URL	Specify a redirect URL if you want to redirect the users to another URL.

In the CLI

To configure an external Captive Portal profile:

```
(Instant AP)(config)# wlan external-captive-portal [profile_name]
(Instant AP)(External Captive Portal)# server <server>
(Instant AP)(External Captive Portal)# port <port>
(Instant AP)(External Captive Portal)# url <url>
(Instant AP)(External Captive Portal)# https
(Instant AP)(External Captive Portal)# redirect-url <url>
(Instant AP)(External Captive Portal)# server-fail-through
(Instant AP)(External Captive Portal)# no auto-whitelist-disable
(Instant AP)(External Captive Portal)# end
(Instant AP)# commit apply
```

Configuring an SSID or Wired Profile to Use External Captive Portal Authentication

You can configure external captive portal authentication for a network profile when adding or editing a guest network using the Instant UI or CLI.

In the Instant UI

1. Navigate to the WLAN wizard or Wired window.
- To configure external captive portal authentication for a WLAN SSID, in the **Network** tab, click **New** to create a new network profile or **edit** to modify an existing profile.
- To configure external captive portal authentication for a wired profile, click **More**>**Wired**. In the **Wired** window, click **New** under **Wired Networks** to create a new network, or click **Edit** to select an existing profile.
2. In the **Security** tab, select **External** from the **Splash page type** drop-down list.
3. From the captive portal profile drop-down list, select a profile. You can select a default profile, or an already existing profile, or click **New** and create a new profile.
4. Configure the following parameters based on the type of splash page you selected.

Table 26: *External Captive Portal Configuration Parameters*

Parameter	Description
WISPr	Select **Enabled** if you want to enable WISPr authentication. For more information on WISPr authentication, see Configuring WISPr Authentication on page 170. **NOTE:** The WISPr authentication is applicable only for the External - RADIUS Server and Internal-Authenticated splash pages and is not applicable for wired profiles.
MAC authentication	Select **Enabled** if you want to enable MAC authentication. For information on MAC authentication, see Configuring MAC Authentication for a Network Profile on page 165.
Authentication server	To configure an authentication server, select any of the following options: • If the server is already configured, select the server from the list. • To create new external RADIUS server, select **New**. For more information, see Configuring an External Server for Authentication on page 157.
Reauth interval	Specify a value for the reauthentication interval at which the APs periodically reauthenticate all associated and authenticated clients.
Accounting mode	Select an accounting mode from **Accounting mode** for posting accounting information at the specified **Accounting interval**. When the accounting mode is set to **Authentication**, the accounting starts only after client authentication is successful and stops when the client logs out of the network. If the accounting mode is set to **Association**, the accounting starts when the client associates to the network successfully and stops when the client is disconnected.
Blacklisting	If you are configuring a wireless network profile, select **Enabled** to enable blacklisting of the clients with a specific number of authentication failures.
Max authentication failures	If you are configuring a wireless network profile and the **Blacklisting** is enabled, specify a maximum number of authentication failures after which users who fail to authenticate must be dynamically blacklisted.

Table 26: *External Captive Portal Configuration Parameters*

Parameter	Description
Walled garden	Click the link to open the **Walled Garden** window. The walled garden configuration determines access to the websites. For more information, see Configuring Walled Garden Access on page 138.
Disable if uplink type is	Select the type of the uplink to exclude.
Encryption	Select Enabled to configure encryption settings and specify the encryption parameters.

5. Click **Next** to continue and then click **Finish** to apply the changes.

In the CLI

To configure security settings for guest users of the WLAN SSID profile:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# essid <ESSID-name>
(Instant AP)(SSID Profile <name>)# type <Guest>
(Instant AP)(SSID Profile <name>)# captive-portal{<type>[exclude-uplink <types>]| external
[exclude-uplink <types>| profile <name>[exclude-uplink <types>]]}
(Instant AP)(SSID Profile <name>)# blacklist
(Instant AP)(SSID Profile <name>)# mac-authentication
(Instant AP)(SSID Profile <name>)# max-authentication-failures <number>
(Instant AP)(SSID Profile <name>)# auth-server <server-name>
(Instant Access Point (SSID Profile <name>)# radius-accounting
(Instant Access Point (SSID Profile <name>)# radius-interim-accounting-interval
(Instant Access Point (SSID Profile <name>)# radius-accounting-mode {user-association|user-
authentication}
(Instant AP)(SSID Profile <name>)# wpa-passphrase <WPA_key>
(Instant AP)(SSID Profile <name>)# wep-key <WEP-key> <WEP-index>
(Instant AP)(SSID Profile <name>)# end
(Instant AP)# commit apply
```

To configure security settings for guest users of the wired profile:

```
(Instant AP)(config)# wired-port-profile <name>
(Instant AP)(wired ap profile <name>)# type <Guest>
(Instant AP)(wired ap profile <name>)# captive-portal{<type>[exclude-uplink <types>]| external
[exclude-uplink <types>| profile <name>[exclude-uplink <types>]]}
(Instant AP)(wired ap profile <name>)# mac-authentication
(Instant AP)(wired ap profile <name>)# end
(Instant AP)# commit apply
```

Configuring External Captive Portal Authentication Using ClearPass Guest

You can configure Instant to point to ClearPass Guest as an external Captive Portal server. With this configuration, the user authentication is performed by matching a string in the server response and RADIUS server (either ClearPass Guest or a different RADIUS server).

Creating a Web Login page in ClearPass Guest

The ClearPass Guest Visitor Management Appliance provides a simple and personalized user interface through which operational staff can quickly and securely manage visitor network access. With ClearPass Guest, the users can have a controlled access to a dedicated visitor management user database. Through a customizable Web portal, the administrators can easily create an account, reset a password or set an expiry time for visitors. Visitors can be registered at reception and provisioned with an individual guest account that defines their visitor profile and the duration of their visit. By defining a Web login page on the ClearPass Guest Visitor Management Appliance, you are able to provide a customized graphical login page for visitors accessing the network.

For information on setting up the RADIUS Web Login feature, see the *RADIUS Services* section in the **ClearPass Guest Deployment Guide**.

Configuring RADIUS Server in Instant UI

To configure Instant to point to ClearPass Guest as an external Captive Portal server, perform the following steps:

1. Select the WLAN SSID for which you want to enable external captive portal authentication with CPPM. You can also configure the RADIUS server when configuring a new SSID profile.
2. In the **Security** tab, select **External** from the Splash page type.
3. Select **New** from the **Captive portal profile** drop-down list and update the following fields:
   a. Enter the IP address of the ClearPass Guest server in the **IP or hostname** field. Obtain the ClearPass Guest IP address from your system administrator.
   b. Enter **/page_name.php** in the **URL** field. This URL must correspond to the **Page Name** configured in the ClearPass Guest RADIUS Web Login page. For example, if the Page Name is **Dell**, the URL should be **/Dell.php** in the Instant UI**.**
   c. Enter the **Port** number (generally should be **80**). The ClearPass Guest server uses this port for HTTP services.
   d. Click **OK**.
4. To create an external RADIUS server, select **New** from the **Authentication server 1** drop-down list. For information on authentication server configuration parameters, see Configuring an External Server for Authentication on page 157.
5. Click **Next** and then click **Finish**.
6. Click the updated SSID in the Network tab.
7. Open any browser and type any URL. Instant redirects the URL to ClearPass Guest login page.
8. Log in to the network with the user name and password specified used while configuring the RADIUS server.

Configuring Guest Logon Role and Access Rules for Guest Users

For captive portal profile, you can create any the following types of roles:

- A pre-authenticated role - This role is assigned before the captive portal authentication. The user can only access certain destinations with this role.
- A guest role - This role is assigned after user authentication.
- A captive-portal role - This role can be assigned to any network such as empolyee, voice, or guest. When the user is assigned with this role, a splash page is displayed after opening a browser and the users may need to authenticate.

You can configure up to 128 access rules for guest user roles through the Instant UI or CLI.

In the Instant UI

To configure roles and access rules for the guest network:

1. In the **Access Rules** tab, set the slider to any of the following types of access control:
   - **Unrestricted**– Select this to set unrestricted access to the network.
   - **Network-based**– Set the slider to **Network-based** to set common rules for all users in a network. The **Allow any to all destinations** access rule is enabled by default. This rule allows traffic to all destinations. To define an access rule:
     a. Click **New**.
     b. Select appropriate options in the **New Rule** window.
     c. Click **OK**.
   - **Role-based**– Select **Role-based** to enable access based on user roles. For role-based access control:
     - Create a user role if required. For more information, see Configuring User Roles.
     - Create access rules for a specific user role. For more information, see Configuring Access Rules for Network Services on page 177. You can also configure an access rule to enforce captive portal authentication for an SSID with the 802.1X authentication method. For more information, see Configuring Captive Portal Roles for an SSID on page 135.
     - Create a role assignment rule. For more information, see Configuring Derivation Rules on page 192. Instant supports role derivation based on the DHCP option for Captive Portal authentication. When the Captive Portal authentication is successful, a new user role is assigned to the guest users based on DHCP option configured for the SSID profile, instead of the pre-authenticated role.
2. Click **Finish**.

In the CLI

To configure access control rules for a WLAN SSID:

```
(Instant AP)(config)# wlan access-rule <name>
(Instant AP)(Access Rule <name>)# rule <dest> <mask> <match> {<protocol> <start-port> <end-
port> {permit|deny|src-nat|dst-nat{<IP-address> <port>| <port>}}| app <app> {permit| deny}|
appcategory <appgrp>| webcategory <webgrp> {permit| deny}| webreputation <webrep>
[<option1....option9>]
(Instant AP)(Access Rule <name>)# end
(Instant AP)# commit apply
```

To configure access control based on the SSID:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# set-role-by-ssid
(Instant AP)(SSID Profile <name>)# end
(Instant AP)# commit apply
```

To configure role assignment rules:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# set-role <attribute>{{equals|not-equals|starts-with|ends-
with|contains|matches-regular-expression}<operator><role>|value-of}
(Instant AP)(SSID Profile <name>)# end
(Instant AP)# commit apply
```

To configure a pre-authentication role:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# set-role-pre-auth <pre-authentication-role>
(Instant AP)(SSID Profile <name>)# end
(Instant AP)# commit apply
```

To configure machine and user authentication roles

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# set-role-machine-auth <machine-authentication-only> <user-
authentication-only>
```

```
(Instant AP)(SSID Profile <name># end
(Instant AP)# commit apply
```

To configure unrestricted access:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name># set-role-unrestricted
(Instant AP)(SSID Profile <name># end
(Instant AP)# commit apply
```

Example

The following example configures access rules for the wireless network:

```
(Instant AP)(config)# wlan access-rule WirelessRule
(Instant AP)(Access Rule "WirelessRule")# rule 192.0.2.2 255.255.255.0 match 6 4343 4343 log
classify-media
(Instant AP)(Access Rule "WirelessRule")# rule any any match app deny throttle-downstream 256
throttle-up 256
(Instant AP)(Access Rule "WirelessRule")# rule any any match appcategory collaboration permit
(Instant AP)(Access Rule "WirelessRule")# rule any any match webcategory gambling deny
(Instant AP)(Access Rule "WirelessRule")# rule any any match webcategory training-and-tools
permit
(Instant AP)(Access Rule "WirelessRule")# rule any any match webreputation well-known-sites
permit
(Instant AP)(Access Rule "WirelessRule")# rule any any match webreputation safe-sites permit
(Instant AP)(Access Rule "WirelessRule")# rule any any match webreputation benign-sites permit
(Instant AP)(Access Rule "WirelessRule")# rule any any match webreputation suspicious-sites
deny
(Instant AP)(Access Rule "WirelessRule")# rule any any match webreputation high-risk-sites
deny
(Instant AP)(Access Rule "WirelessRule")# end
(Instant AP)# commit apply
```

Configuring Captive Portal Roles for an SSID

You can configure an access rule to enforce captive portal authentication for SSIDs with 802.1X authentication enabled. You can configure rules to provide access to an external captive portal, internal captive portal, so that some of the clients using this SSID can derive the captive portal role.

The following conditions apply to the 802.1X and captive portal authentication configuration:

- If a user role does not have Captive Portal settings configured, the captive portal settings configured for an SSID are applied to the client's profile.
- If the SSID does not have Captive Portal settings configured, the captive portal settings configured for a user role are applied to the client's profile.
- If captive portal settings are configured for both SSID and user role, the captive portal settings configured for a user role are applied to the client's profile.

You can create a captive portal role for both **Internal-acknowledged** and **External Authentication Text** splash page types.

To enforce the Captive Portal role, use the Instant UI or CLI.

In the Instant UI

To create a captive portal role:

1. Select an SSID profile from the **Networks** tab. The **Edit <WLAN-Profile>** window is displayed.
2. In the **Access** tab, slide to **Role-based** access control by using the scroll bar.
3. Select a role or create a new one if required.

4. Click **New** to add a new rule. The **New Rule** window is displayed.
5. In the **New Rule** window, specify the following parameters. The following figures show the parameters for Captive Portal role configuration:

Figure 40 *Captive Portal Rule for Internal Acknowledged Splash Page*

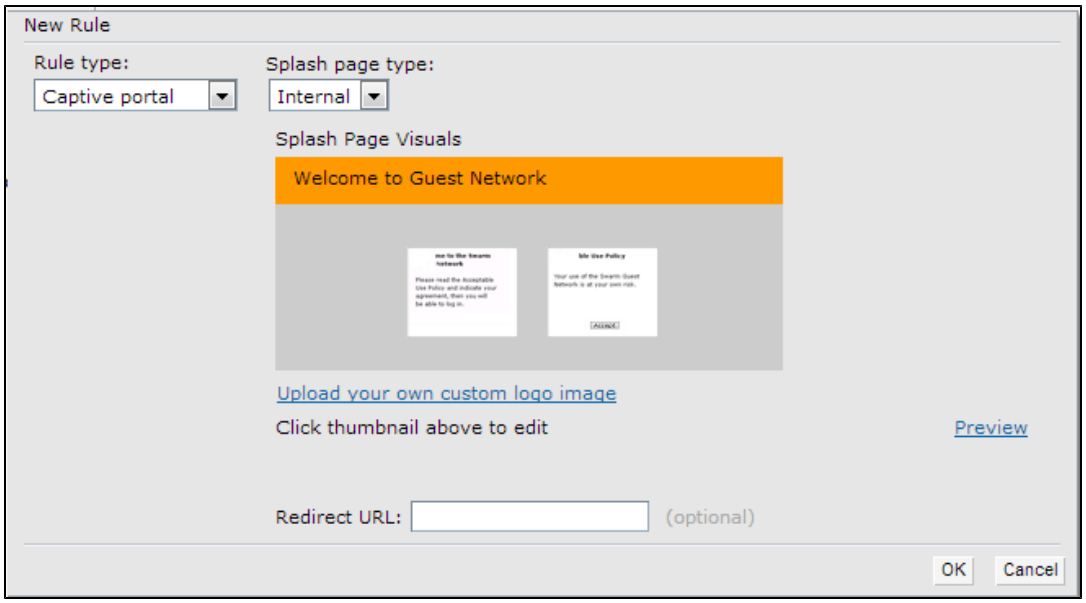


Figure 41 *Captive Portal Rule for External Captive portal profile*

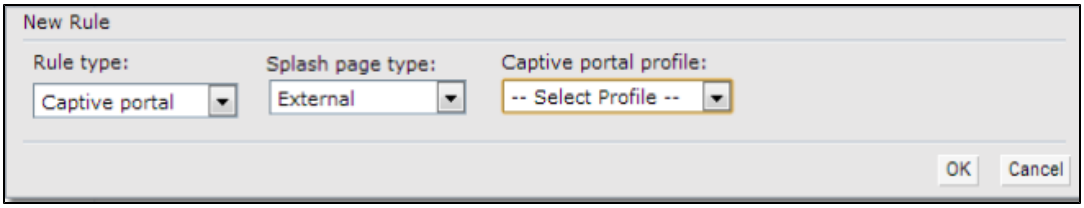


Table 27: *New Access Rule Configuration Parameters*

Field	Description
Rule type	Select **Captive Portal** from the drop-down list.
Splash Page Type	Select any of following attributes: • Select **Internal** to configure a rule for internal captive portal authentication. • Select **External** to configure a rule for external captive portal authentication.
Internal	If **Internal** is selected as splash page type, perform the following steps: • Under **Splash Page Visuals**, use the editor to specify text and colors for the initial page that would be displayed to users connecting to the network. The initial page asks for user credentials or email, depending on the splash page type configured • To change the color of the splash page, click the Splash page rectangle and select the required color from the **Background Color** palette. • To change the welcome text, click the first square box in the splash page, type the required text in the **Welcome** text box, and click **OK**. Ensure that the welcome text does not exceed 127 characters.

Field	Description
	• To change the policy text, click the second square in the splash page, type the required text in the **Policy** text box, and click **OK**. Ensure that the policy text does not exceed 255 characters. • Specify the URL to which you want to redirect the guest users. • To upload a custom logo, click **Upload your own custom logo Image**, browse the image file, and click **upload image**. • Click **Preview** to preview the Captive Portal page.

External	If **External** is selected, perform the following steps:
	• Select a profile from the **Captive portal profile** drop-down list.
	• If you want to edit the profile, click **Edit** and update the following parameters:
	  • **Type**–Select either **Radius Authentication** (to enable user authentication against a RADIUS server) or **Authentication Text** (to specify the authentication text to returned by the external server after a successful user authentication).
	  • **IP or hostname**– Enter the IP address or the hostname of the external splash page server.
	  • **URL**– Enter the URL for the external splash page server.
	  • **Port**–Enter the number of the port to use for communicating with the external splash page server
	  • **Redirect URL**–Specify a redirect URL if you want to redirect the users to another URL.
	  • **Captive Portal failure**–This field allows you to configure Internet access for the guest clients when the external captive portal server is not available. Select **Deny Internet** to prevent clients from using the network, or **Allow Internet** to allow the guest clients to access Internet when the external captive portal server is not available.
	  • **Automatic URL Whitelisting**– Select **Enabled** or **Disabled** to enable or disable automatic whitelisting of URLs. On selecting the checkbox for the external captive portal authentication, the URLs allowed for the unauthenticated users to access are automatically whitelisted. The automatic URL whitelisting is disabled by default.
	  • **Auth Text**–Indicates the authentication text returned by the external server after a successful user authentication.

6. Click **OK**. The enforce captive portal rule is created and listed as an access rule.
7. Create a role assignment rule based on the user role, to which the captive portal access rule is assigned.
8. Click **Finish**.

The client can connect to this SSID after authenticating with username and password. After a successful user login, the captive portal role is assigned to the client.

In the CLI

To create a captive portal role:

```
(Instant AP)(config)# wlan access-rule <Name>
(Instant AP)(Access Rule <Name>)# captive-portal {external [profile <name>]|internal}
(Instant AP)(Access Rule <Name>)# end
(Instant AP)# commit apply
```

Configuring Walled Garden Access

On the Internet, a walled garden typically controls access to Web content and services. The Walled garden access is required when an external captive portal is used. For example, a hotel environment where the unauthenticated users are allowed to navigate to a designated login page (for example, a hotel website) and all its contents.

The users who do not sign up for the Internet service can view the “allowed” websites (typically hotel property websites). The website names must be DNS-based and support the option to define wildcards. This works for client devices with or without HTTP proxy settings.

When a user attempts to navigate to other websites, which are not in the whitelist of the walled garden profile, the user is redirected to the login page. In addition, a blacklisted walled garden profile can also be configured to explicitly block the unauthenticated users from accessing some websites.

You can create a walled garden access in Instant UI or CLI.

In the Instant UI

To create a Walled Garden access:

1. Click the **Security** link at the top right corner of the Instant main window and click **Walled Garden**. The Walled Garden tab contents are displayed.
2. To allow users to access a specific domain, click **New** and enter the domain name or URL in the **Whitelist** section of the window. This allows access to a domain while the user remains unauthenticated. Specify a POSIX regular expression (regex(7)). For example:
   - yahoo.com matches various domains such as news.yahoo.com, travel.yahoo.com and finance.yahoo.com
   - www.apple.com/library/test is a subset of **apple.com** site corresponding to path /library/test/*
   - favicon.ico allows access to /favicon.ico from all domains.
3. To deny users access to a domain, click **New** and enter the domain name or URL in the **Blacklist** section of the window. This prevents the unauthenticated users from viewing specific websites. When a URL specified in the blacklist is accessed by an unauthenticated user, W-IAP sends an HTTP 403 response to the client with a simple error message.

   If the requested URL does not appear on the blacklist or whitelist list, the request is redirected to the external captive portal.
4. Select the domain name/URL and click **Edit** to modify or **Delete** to remove the entry from the list.
5. Click **OK** to apply the changes.

In the CLI

To create a Walled Garden access:

```
(Instant AP)(config)# wlan walled-garden
(Instant AP)(Walled Garden)# white-list <domain>
(Instant AP)(Walled Garden)# black-list <domain>
(Instant AP)(Walled Garden)# end
(Instant AP)# commit apply
```

Disabling Captive Portal Authentication

To disable captive portal authentication, perform the following steps:

1. Select an existing wireless or wired profile. Depending on the network profile selected, the **Edit <WLAN-Profile>** or **Edit Wired Network** window is displayed.

You can also customize splash page design in the **Security** tab of **New WLAN** and **New Wired Network** windows when configuring a new profile.

2. Navigate to the **Security** tab.
3. Select **None** from the **Splash page type** drop-down list.
4. Click **Next** and then click **Finish** to apply the changes.

This chapter provides the following information:

- Managing W-IAP Users on page 140
- Understanding Authentication Methods on page 147
- Supported Authentication Servers on page 149
- Understanding Encryption Types on page 154
- Support for Authentication Survivability on page 155
- Configuring Authentication Servers on page 157
- Configuring 802.1X Authentication for a Network Profile on page 163
- Configuring MAC Authentication for a Network Profile on page 165
- Configuring MAC Authentication with 802.1X Authentication on page 167
- Configuring MAC Authentication with Captive Portal Authentication on page 169
- Configuring WISPr Authentication on page 170
- Blacklisting Clients on page 171
- Uploading Certificates on page 173

Managing W-IAP Users

The W-IAP users can be classified as follows:

- Administrator– An admin user who creates SSIDs, wired profiles, DHCP server configuration parameters, and manages the local user database. The admin users can access to the Virtual Controller Management User Interface.
- Guest administrator– A guest interface management user who manages guest users added in the local user database.
- Administrator with read-only access– The read-only admin user does not have access to the Instant CLI. The Instant UI will be displayed in the read-only mode for these users.
- Employee users – Employees who use the enterprise network for official tasks.
- Guest users–Visiting users who temporarily use the enterprise network to access the Internet.

The user access privileges are determined by W-IAP management settings in the W-AirWave Management client, and the type of the user. The following table outlines the access privileges defined for the admin user, guest management interface admin, and read-only users.

Table 28: *User Privileges*

User Category	W-AirWave Management Platform in Management Mode	W-IAP in monitor mode or without W-AirWave Management Platform
administrator	Access to local user database only	Complete access to the W-IAP
read-only administrator	No write privileges	No write privileges
guest administrator	Access to local user database only	Access to local user database only

Configuring Authentication Parameters for Management Users

Instant now allows you to configure a TACACS+ Server as the authentication server to support authentication and accounting privileges for management users. TACACS+ server allows a remote access server to communicate with an authentication server to determine if the user has access to the network. In Instant, the users can create several TACACS+ server profiles, out of which one or two of the servers can be specified to authenticate management users.

TACACS+ supports the following types of authentication for management users in Instant:

- ASCII
- PAP
- CHAP
- ARAP
- MSCHAP

The TACACS+ server cannot be attributed to any SSID or wired profile in general as the authentication server and is configured only for management users.

You can also enable TACACS+ accounting when the TACACS+ server is used for authentication.

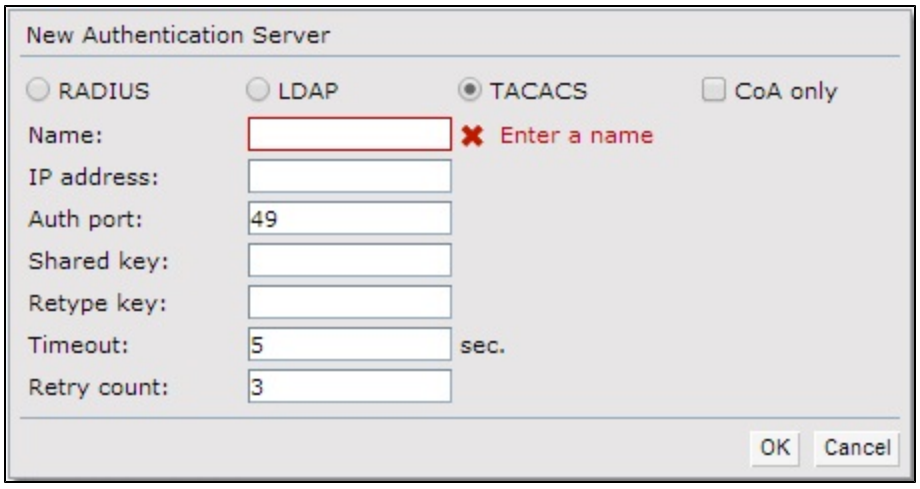
Configuring a TACACS+ Server Profile for Management User Authentication

To configure a TACACS+ authentication server:

In the Instant UI

1. Navigate to **Security**>**Authentication Servers**. The **Security** window is displayed.
2. To create a new server, click **New**. A window for configuring server details for the new server is displayed. The following figure shows the parameters to configure for a new authentication server configuration:

Figure 42 *New Authentication Server Window*



To create a TACACS+ server profile, specify the attributes described in the following table:

Table 29: *TACACS+ Server Configuration Parameters*

Parameter	Description
IP address	Enter the IP address of the TACACS+ server.
Auth Port	Enter the TCP IP port used by the server. The default port number is 49.
Shared Key	Enter the secret key of your choice to authenticate communication between the TACACS+ client and server.
Retype Key	Re-enter the secret key you have specified as the Shared Key.
Timeout	Enter a number between 1 and 30 seconds to indicate the timeout period for TACACS+ requests. The default value is 20 seconds.
Retry Count	Enter a number between 1 and 5 to indicate the maximum number of authentication attempts. The default value is 3.

In the CLI

To configure a TACACS+ server:

```
(Instant AP)(config)# wlan tacacs-server <profile-name>
(Instant AP)(TACACS Server <profile-name>)# ip <IP-address>
(Instant AP)(TACACS Server <profile-name>)# port <port>
(Instant AP)(TACACS Server <profile-name>)# key <key>
(Instant AP)(TACACS Server <profile-name>)# timeout <seconds>
(Instant AP)(TACACS Server <profile-name>)# retry-count <number>
(Instant AP)(TACACS Server <profile-name>)# deadtime <minutes>
(Instant AP)(TACACS Server <profile-name>)# end
```

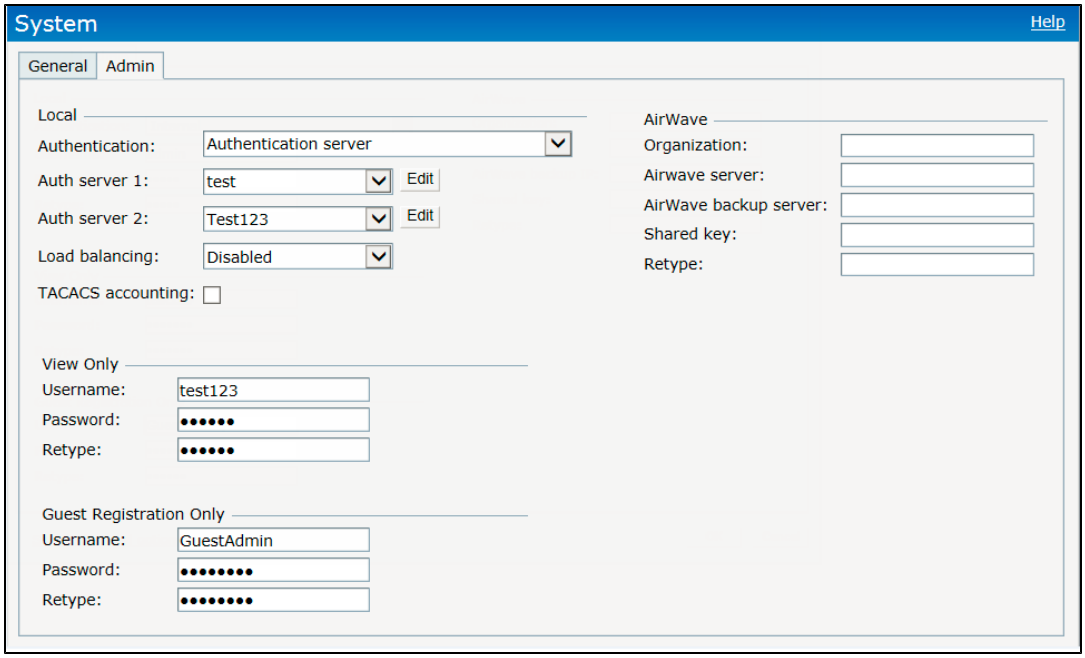
Configuring Administrator Credentials for the Virtual Controller Interface

You can configure authentication parameters for admin users to enable access to the Virtual Controller management user interface in the Instant UI or CLI.

In the Instant UI

1. Click the **System** link at top right corner of the Instant main window. The **System** window is displayed.
2. Click the **Admin** tab. The **Admin** tab details are displayed. The following figure shows the contents of the **Admin** tab:

Figure 43 *Admin Tab: Management Authentication Parameters*



3. Under Local, select any of the following options from the **Authentication** drop-down list:

- **Internal**– Select this option to specify a single set of user credentials. Enter the **Username** and **Password** for accessing the Virtual Controller Management User Interface.
- **Authentication Server**– Specify one or two authentication servers to authenticate clients. If two servers are configured, users can use them in primary or backup mode or load balancing mode. To enable load balancing, select **Enabled** from the **Load balancing** drop-down list. For more information on load balancing, see Dynamic Load Balancing between Two Authentication Servers on page 154.

  You may also specify a RADIUS Server as one of the authentication servers along with a TACACS+ server. If a TACACS+ server is selected, you can select the TACACS accounting checkbox for reporting management commands.

The **TACACS accounting** option is available only when a TACACS+ server is specified as one of the authentication servers.

- **Authentication server w/ fallback to internal**– Select this option to use both internal and external servers. When enabled, the authentication switches to **Internal** if there is no response from the RADIUS server (RADIUS server timeout). To complete this configuration, perform the following step:
  a. To enable load balancing, select **Enabled** from the **Load balancing** drop-down list.
  b. Specify a **Username** and **Password**.
  c. Retype the password to confirm.

4. Click **OK**.

In the CLI

To configure an admin user:

```
(Instant AP)(config)# mgmt-user <username> [password]
(Instant AP)(config)# end
(Instant AP)# commit apply
```

To configure RADIUS or TACACS+ authentication parameters:

```
(Instant AP)(config)# mgmt-auth-server <authentication_server1>
```

```
(Instant AP)(config)# mgmt-auth-server <authentication_server2>
(Instant AP)(config)# mgmt-auth-server-load-balancing
(Instant AP)(config)# mgmt-auth-server-local-backup
(Instant AP)(config)# end
(Instant AP)# commit apply
```

To configure management authentication settings:

```
(Instant AP)(config)# mgmt-auth-server <server1>
(Instant AP)(config)# mgmt-auth-server <server2>
(Instant AP)(config)# mgmt-auth-server-load-balancing
(Instant AP)(config)# mgmt-auth-server-local-backup
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Configuring Guest Management Interface Administrator Credentials

You can configure guest administrator credentials in the Instant UI or CLI.

In the Instant UI

1. Click the **System** link at top right corner of the Instant main window. The **System** window is displayed.
2. Click the **Admin** tab. The **Admin** tab details are displayed.
3. Under **Guest Registration Only**:
   a. Specify a **Username** and **Password**.
   b. Retype the password to confirm.
4. Click **OK**. When the guest management administrator logs in with these credentials, the guest management interface is displayed.

In the CLI

To configure guest management administrator credentials:

```
(Instant AP)(config)# mgmt-user <username> [password] guest-mgmt
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Configuring Users for Internal Database of a W-IAP

The Instant user database consists of a list of guest and employee users. The addition of a user involves specifying a login credentials for a user. The login credentials for these users are provided outside the Instant system.

A guest user can be a visitor who is temporarily using the enterprise network to access the Internet. However, if you do not want to allow access to the internal network and the Intranet, you can segregate the guest traffic from the enterprise traffic by creating a guest WLAN and specifying the required authentication, encryption, and access rules.

An employee user is the employee who is using the enterprise network for official tasks. You can create Employee WLANs, specify the required authentication, encryption and access rules and allow the employees to use the enterprise network.

The user database is also used when a W-IAP is configured as an internal RADIUS server.

The local user database of APs can support up to 512 user entries except W-IAP9x. W-IAP9x supports only 256 user entries. If there are already 512 users, W-IAP9x will not be able to join the cluster.

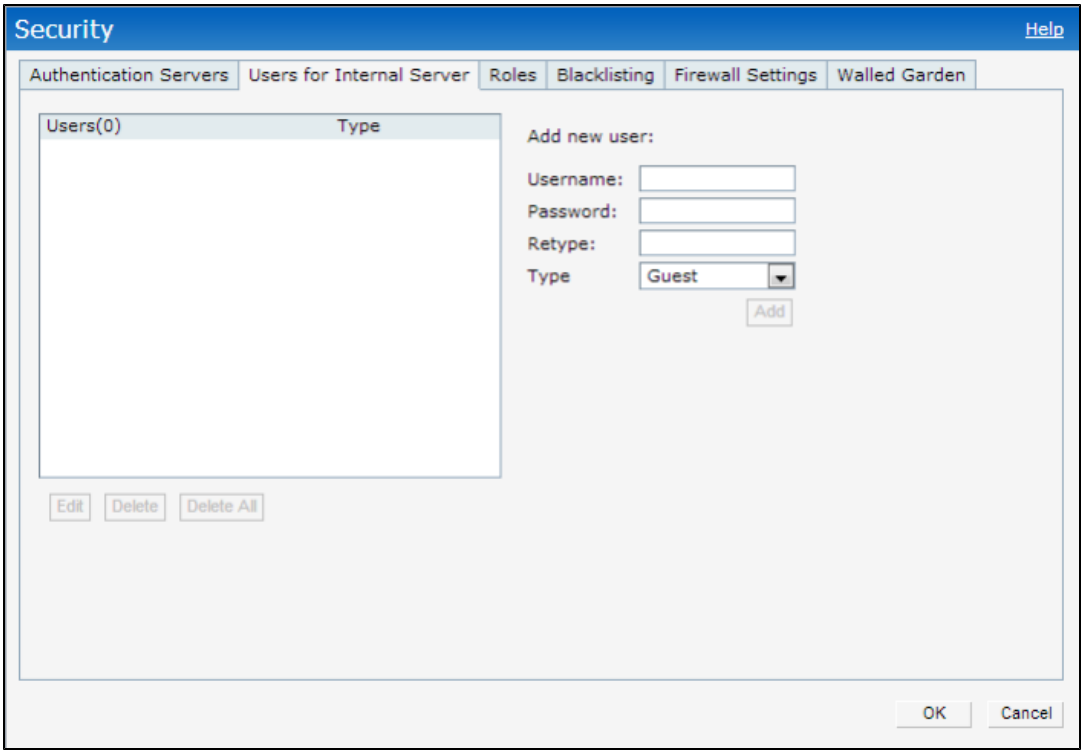
In the Instant UI

To configure users:

1. Click the **Security** at the top right corner of Instant main window.

2. Click **Users for Internal Server**. The following figure shows the contents of the **Users for Internal Server** tab.

Figure 44 *Adding a User*



3. Enter the username in the **Username** text box.
4. Enter the password in the **Password** text box and reconfirm.
5. Select a type of network from the **Type** drop-down list.
6. Click **Add** and click **OK.** The users are listed in the **Users** list.
7. To edit user settings:
   a. Select the user to modify under **Users**
   b. Click **Edit** to modify user settings.
   c. Click **OK**.
8. To delete a user:
   a. In the **Users** section, select the username to delete
   b. Click **Delete**.
   c. Click **OK**.
9. To delete all or multiple users at a time:
   a. Select the usernames that you want to delete
   b. Click **Delete All**.
   c. Click **OK**.

Deleting a user only removes the user record from the user database, and will not disconnect the online user associated with the username.

In the CLI

To configure an employee user:

```
(Instant AP)(config)# user <username> <password> radius
(Instant AP)(config)# end
```

```
(Instant AP)# commit apply
```

To configure a guest user:

```
(Instant AP)(config)# user <username> <password> portal
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Configuring the Read-Only Administrator Credentials

You can assign the read-only privilege to an admin user by using the Instant UI or CLI.

In the Instant UI

1. Click the **System** link at top right corner of the Instant main window. The **System** window is displayed.
2. Click the **Admin** tab. The **Admin** tab details are displayed.
3. Under **View Only**:
   a. Specify a **Username** and **Password**.
   b. Retype the password to confirm.
4. Click **OK**. When the users log in with these credentials, the Instant UI is displayed in the read-only mode.

In the CLI

To configure a user with read-only privilege:

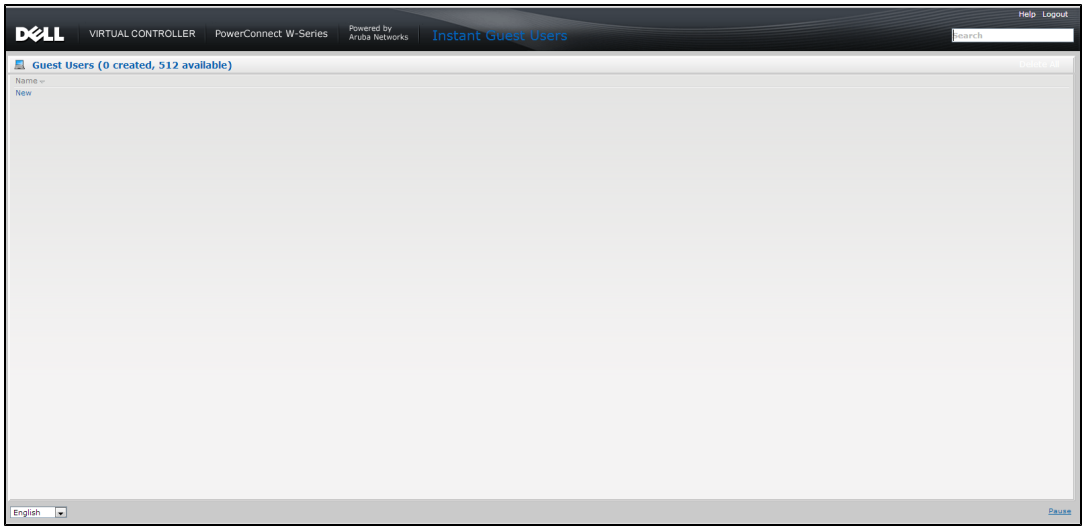
```
(Instant AP)(config)# mgmt-user <username> [password] read-only
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Adding Guest Users through the Guest Management Interface

To add guest users through the Guest Management interface:

1. Log in to Instant UI with the guest management interface administrator credentials. The guest management interface is displayed.

Figure 45 *Guest Management Interface*



2. To add a user, click **New**. The **New Guest User** pop-up window is displayed.
3. Specify a **Username** and **Password**.
4. Retype the password to confirm.
5. Click **OK**.

Understanding Authentication Methods

Authentication is a process of identifying a user by through a valid username and password or based on their MAC addresses. The following authentication methods are supported in Instant:

- 802.1X authentication
- MAC authentication
- MAC authentication with 802.1X authentication
- Captive Portal Authentication
- MAC authentication with Captive Portal authentication
- 802.1X authentication with Captive Portal Role
- WISPr authentication

802.1X authentication

802.1X is an IEEE standard that provides an authentication framework for WLANs. 802.1x uses the Extensible Authentication Protocol (EAP) to exchange messages during the authentication process. The authentication protocols that operate inside the 802.1X framework include EAP-Transport Layer Security (EAP-TLS), Protected EAP (PEAP), and EAP-Tunneled TLS (EAP-TTLS). These protocols allow the network to authenticate the client while also allowing the client to authenticate the network. For more information on EAP authentication framework supported by the W-IAP, see Supported EAP Authentication Frameworks on page 148.

802.1X authentication method allows a W-IAP to authenticate the identity of a user before providing network access to the user. The Remote Authentication Dial In User Service (RADIUS) protocol provides centralized authentication, authorization, and accounting management. For authentication purpose, the wireless client can associate to a network access server (NAS) or RADIUS client such as a wireless W-IAP. The wireless client can pass data traffic only after successful 802.1X authentication.

For more information on configuring a W-IAP to use 802.1X authentication, see Configuring 802.1X Authentication for a Network Profile on page 163.

MAC authentication

MAC authentication is used for authenticating devices based on their physical MAC addresses. MAC authentication requires that the MAC address of a machine matches a manually defined list of addresses. This authentication method is not recommended for scalable networks and the networks that require stringent security settings. For more information on configuring a W-IAP to use MAC authentication, see Configuring MAC Authentication for a Network Profile on page 165.

MAC authentication with 802.1X authentication

This authentication method has the following features:

- MAC authentication precedes 802.1X authentication - The administrators can enable MAC authentication for 802.1X authentication. MAC authentication shares all the authentication server configurations with 802.1X authentication. If a wireless or wired client connects to the network, MAC authentication is performed first. If MAC authentication fails, 802.1X authentication does not trigger. If MAC authentication is successful, 802.1X authentication is attempted. If 802.1X authentication is successful, the client is assigned an 802.1X authentication role. If 802.1X authentication fails, the client is assigned a **deny-all** role or **mac-auth-only** role.
- MAC authentication only role - Allows you to create a **mac-auth-only** role to allow role-based access rules when MAC authentication is enabled for 802.1X authentication. The **mac-auth-only** role is assigned to a client when the MAC authentication is successful and 802.1X authentication fails. If 802.1X authentication is successful, the **mac-auth-only** role is overwritten by the final role. The **mac-auth-only** role is primarily used for wired clients.

- L2 authentication fall-through - Allows you to enable the **l2-authentication-fallthrough** mode. When this option is enabled, the 802.1X authentication is allowed even if the MAC authentication fails. If this option is disabled, 802.1X authentication is not allowed. The **l2-authentication-fallthrough** mode is disabled by default.

  For more information on configuring a W-IAP to use MAC + 802.1X Authentication, see Configuring MAC Authentication with 802.1X Authentication on page 167.

Captive Portal Authentication

Captive portal authentication is used for authenticating guest users. For more information on Captive Portal authentication, see Captive Portal for Guest Access on page 120.

MAC authentication with Captive Portal authentication

This authentication method has the following features:

- If the captive portal splash page type is **Internal-Authenticated** or **External-RADIUS Server**, MAC authentication reuses the server configurations.
- If the captive portal splash page type is **Internal-Acknowledged** or **External-Authentication Text** and MAC authentication is enabled, a server configuration page is displayed.
- If the captive portal splash page type is **none**, MAC authentication is disabled.
- You can configure the **mac-auth-only** role when MAC authentication is enabled with captive portal authentication.

For more information configuring a W-IAP to use MAC and Captive Portal authentication, see Configuring MAC Authentication with Captive Portal Authentication on page 169.

802.1X authentication with Captive Portal Role

This authentication mechanism allows you to configure different captive portal settings for clients on the same SSID. For example, you can configure an 802.1x SSID and create a role for captive portal access, so that some of the clients using the SSID derive the captive portal role. You can configure rules to indicate access to external or internal captive portal, or none. For more information on configuring captive portal roles for an SSID with 802.1x authentication, see Configuring Captive Portal Roles for an SSID on page 135.

WISPr authentication

Wireless Internet Service Provider roaming (WISPr) authentication allows a smart client to authenticate on the network when they roam between wireless Internet service providers, even if the wireless hotspot uses an Internet Service Provider (ISP) with whom the client may not have an account.

If a hotspot is configured to use WISPr authentication in a specific ISP and a client attempts to access the Internet at that hotspot, the WISPr AAA server configured for the ISP authenticates the client directly and allows the client to access the network. If the client only has an account with a *partner* ISP, the WISPr AAA server forwards the client's credentials to the partner ISP's WISPr AAA server for authentication. When the client is authenticated on the partner ISP, it is also authenticated on your hotspot's own ISP as per their service agreements. The W-IAP assigns the default WISPr user role to the client when your ISP sends an authentication message to the W-IAP. For more information on WISPr authentication, see Configuring WISPr Authentication on page 170.

Supported EAP Authentication Frameworks

The following EAP authentication frameworks are supported in the Instant network:

- EAP-TLS– The Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) method supports the termination of EAP-TLS security using the internal RADIUS server . The EAP-TLS requires both server and certification authority (CA) certificates installed on the W-IAP. The client certificate is verified on the Virtual

Controller (the client certificate must be signed by a known CA), before the username is verified on the authentication server.

- EAP-TTLS (MSCHAPv2)– The Extensible Authentication Protocol-Tunneled Transport Layer Security (EAP-TTLS) method uses server-side certificates to set up authentication between clients and servers. However, the actual authentication is performed using passwords.
- EAP-PEAP (MSCHAPv2)– EAP-PEAP is an 802.1X authentication method that uses server-side public key certificates to authenticate clients with server. The PEAP authentication creates an encrypted SSL / TLS tunnel between the client and the authentication server. Exchange of information is encrypted and stored in the tunnel ensuring the user credentials are kept secure.
- LEAP– Lightweight Extensible Authentication Protocol (LEAP) uses dynamic WEP keys for authentication between the client and authentication server.

To use the W-IAP's internal database for user authentication, add the names and passwords of the users to be authenticated.

Dell does not recommend the use of LEAP authentication, because it does not provide any resistance to network attacks.

Authentication Termination on W-IAP

W-IAPs support EAP termination for enterprise WLAN SSIDs. The EAP termination can reduce the number of exchange packets between the W-IAP and the authentication servers. Instant allows Extensible Authentication Protocol (EAP) termination for Protected Extensible Authentication Protocol (PEAP)-Generic Token Card (PEAP-GTC) and Protected Extensible Authentication Protocol-Microsoft Challenge Authentication Protocol version 2 (PEAP-MSCHAV2). PEAP-GTC termination allows authorization against an Lightweight Directory Access Protocol (LDAP) server and external RADIUS server while PEAP-MSCHAV2 allows authorization against an external RADIUS server.

This allows the users to run PEAP-GTC termination with their username and password to a local Microsoft Active Directory server with LDAP authentication.

- EAP-Generic Token Card (GTC)– This EAP method permits the transfer of unencrypted usernames and passwords from client to server. The main uses for EAP-GTC are one-time token cards such as SecureID and the use of LDAP or RADIUS as the user authentication server. You can also enable caching of user credentials on the W-IAP to an external authentication server for user data backup.
- EAP-Microsoft Challenge Authentication Protocol version 2 (MS-CHAPv2)– This EAP method is widely supported by Microsoft clients. A RADIUS server must be used as the back-end authentication server.

Supported Authentication Servers

Based on the security requirements, you can configure internal or external authentication servers. This section describes the types of servers that can be configured for client authentication:

- Internal RADIUS Server on page 150
- External RADIUS Server on page 150
- Dynamic Load Balancing between Two Authentication Servers on page 154

In 6.4.0.2-4.1 release, you can configure TACACS+ server for authenticating management users. For more information, on management users and TACACS+ server based authentication, see Configuring Authentication Parameters for Management Users .

Internal RADIUS Server

Each W-IAP has an instance of free RADIUS server operating locally. When you enable the internal RADIUS server option for the network, the client on the W-IAP sends a RADIUS packet to the local IP address. The internal RADIUS server listens and replies to the RADIUS packet. Instant itself serves as a RADIUS server for 802.1X authentication. However, the internal RADIUS server can also be configured as a backup RADIUS server for an external RADIUS server.

External RADIUS Server

In the external RADIUS server, the IP address of the Virtual Controller is configured as the NAS IP address. Instant RADIUS is implemented on the Virtual Controller, and this eliminates the need to configure multiple NAS clients for every W-IAP on the RADIUS server for client authentication. Instant RADIUS dynamically forwards all the authentication requests from a NAS to a remote RADIUS server. The RADIUS server responds to the authentication request with an **Access-Accept** or **Access-Reject** message, and the clients are allowed or denied access to the network depending on the response from the RADIUS server. When you enable an external RADIUS server for the network, the client on the W-IAP sends a RADIUS packet to the local IP address. The external RADIUS server then responds to the RADIUS packet.

Instant supports the following external authentication servers:

- RADIUS (Remote Authentication Dial-In User Service)
- LDAP (Lightweight Directory Access Protocol)
- CPPM Server for AirGroup CoA

To use an LDAP server for user authentication, configure the LDAP server on the Virtual Controller, and configure user IDs and passwords. To use a RADIUS server for user authentication, configure the RADIUS server on the Virtual Controller.

RADIUS Server Authentication with VSA

An external RADIUS server authenticates network users and returns to the W-IAP the vendor-specific attribute (VSA) that contains the name of the network role for the user. The authenticated user is placed into the management role specified by the VSA.

Instant supports the following VSAs for user role and VLAN derivation rules:

- AP-Group
- AP-Name
- ARAP-Features
- ARAP-Security
- ARAP-Security-Data
- ARAP-Zone-Access
- Acct-Authentic
- Acct-Delay-Time
- Acct-Input-Gigawords
- Acct-Input-Octets
- Acct-Input-Packets
- Acct-Interim-Interval
- Acct-Link-Count
- Acct-Multi-Session-Id
- Acct-Output-Gigawords
- Acct-Output-Octets

- Acct-Output-Packets
- Acct-Session-Id
- Acct-Session-Time
- Acct-Status-Type
- Acct-Terminate-Cause
- Acct-Tunnel-Packets-Lost
- Add-Port-To-IP-Address
- Aruba-AP-Group
- Aruba-AP-IP-Address
- Aruba-AS-Credential-Hash
- Aruba-AS-User-Name
- Aruba-Admin-Role
- Aruba-AirGroup-Device-Type
- Aruba-AirGroup-Shared-Group
- Aruba-AirGroup-Shared-Role
- Aruba-AirGroup-Shared-User
- Aruba-AirGroup-User-Name
- Aruba-AirGroup-Version
- Aruba-Auth-Survivability
- Aruba-CPPM-Role
- Aruba-Device-Type
- Aruba-Essid-Name
- Aruba-Framed-IPv6-Address
- Aruba-Location-Id
- Aruba-Mdps-Device-Iccid
- Aruba-Mdps-Device-Imei
- Aruba-Mdps-Device-Name
- Aruba-Mdps-Device-Product
- Aruba-Mdps-Device-Profile
- Aruba-Mdps-Device-Serial
- Aruba-Mdps-Device-Udid
- Aruba-Mdps-Device-Version
- Aruba-Mdps-Max-Devices
- Aruba-Mdps-Provisioning-Settings
- Aruba-Named-User-Vlan
- Aruba-Network-SSO-Token
- Aruba-No-DHCP-Fingerprint
- Aruba-Port-Id
- Aruba-Priv-Admin-User
- Aruba-Template-User
- Aruba-User-Group
- Aruba-User-Role

- Aruba-User-Vlan
- Aruba-WorkSpace-App-Name
- Authentication-Sub-Type
- Authentication-Type
- CHAP-Challenge
- Callback-Id
- Callback-Number
- Chargeable-User-Identity
- Class
- Connect-Info
- Connect-Rate
- Crypt-Password
- DB-Entry-State
- Digest-Response
- Domain-Name
- EAP-Message
- Error-Cause
- Event-Timestamp
- Exec-Program
- Exec-Program-Wait
- Expiration
- Fall-Through
- Filter-Id
- Framed-AppleTalk-Link
- Framed-AppleTalk-Network
- Framed-AppleTalk-Zone
- Framed-Compression
- Framed-IP-Address
- Framed-IP-Netmask
- Framed-IPX-Network
- Framed-IPv6-Pool
- Framed-IPv6-Prefix
- Framed-IPv6-Route
- Framed-Interface-Id
- Framed-MTU
- Framed-Protocol
- Framed-Route
- Framed-Routing
- Full-Name
- Group
- Group-Name
- Hint

- Huntgroup-Name
- Idle-Timeout
- Location-Capable
- Location-Data
- Location-Information
- Login-IP-Host
- Login-IPv6-Host
- Login-LAT-Node
- Login-LAT-Port
- Login-LAT-Service
- Login-Service
- Login-TCP-Port
- Menu
- Message-Auth
- NAS-IPv6-Address
- NAS-Port-Type
- Operator-Name
- Password
- Password-Retry
- Port-Limit
- Prefix
- Prompt
- Rad-Authenticator
- Rad-Code
- Rad-Id
- Rad-Length
- Reply-Message
- Requested-Location-Info
- Revoke-Text
- Server-Group
- Server-Name
- Service-Type
- Session-Timeout
- Simultaneous-Use
- State
- Strip-User-Name
- Suffix
- Termination-Action
- Termination-Menu
- Tunnel-Assignment-Id
- Tunnel-Client-Auth-Id
- Tunnel-Client-Endpoint

- Tunnel-Connection-Id
- Tunnel-Medium-Type
- Tunnel-Preference
- Tunnel-Private-Group-Id
- Tunnel-Server-Auth-Id
- Tunnel-Server-Endpoint
- Tunnel-Type
- User-Category
- User-Name
- User-Vlan
- Vendor-Specific

Dynamic Load Balancing between Two Authentication Servers

You can configure two authentication servers to serve as a primary and backup RADIUS server and enable load balancing between these servers. Load balancing of authentication servers ensures that the authentication load is split across multiple authentication servers and enables the W-IAPs to perform load balancing of authentication requests destined to authentication servers such as RADIUS or LDAP.

The load balancing in W-IAP is performed based on outstanding authentication sessions. If there are no outstanding sessions and if the rate of authentication is low, only primary server will be used. The secondary is used only if there are outstanding authentication sessions on the primary server. With this, the load balance can be performed across asymmetric capacity RADIUS servers without the need to obtain inputs about the server capabilities from the administrators.

Understanding Encryption Types

Encryption is the process of converting data into a cryptic format or code when it is transmitted on a network. Encryption prevents unauthorized use of the data.

Instant supports the following types of encryption:

- **WEP** –Wired Equivalent Privacy (WEP) is an authentication method where all users share the same key. WEP is not secure as other encryption types such as TKIP.
- **TKIP** –Temporal Key Integrity Protocol (TKIP) uses the same encryption algorithm as WEP. However, TKIP is more secure and has an additional message integrity check (MIC).
- **AES** – The Advanced Encryption Standard (AES) encryption algorithm a widely supported encryption type for all wireless networks that contain any confidential data. AES in Wi-Fi leverages 802.1X or PSKs to generate per station keys for all devices. AES provides a high level of security like IP Security (IPsec) clients.

WEP and TKIP are limited to WLAN connection speed of 54 Mbps. The 802.11n connection supports only AES encryption. DellIt is recommended to use AES encryption. Ensure that all devices that do not support AES are upgraded or replaced with the devices that support AES encryption.

WPA and WPA2

WPA is created based on a draft of 802.11i, which allowed users to create more secure WLANs. WPA2 encompasses the full implementation of the 802.11i standard. WPA2 is a superset that encompasses the full WPA feature set.

The following table summarizes the differences between the two certifications:

Table 30: *WPA and WPA2 Features*

Certification	Authentication	Encryption
WPA	• PSK • IEEE 802.1X with Extensible Authentication Protocol (EAP)	TKIP with message integrity check (MIC)
WPA2	• PSK • IEEE 802.1X with EAP	AES -- Counter Mode with Cipher Block Chaining Message Authentication Code (AESCCMP)

WPA and WPA2 can be further classified as follows:

- **Personal** – Personal is also called Pre-Shared Key (PSK). In this type, a unique key is shared with each client in the network. Users have to use this key to securely log in to the network. The key remains the same until it is changed by authorized personnel. You can also configure key change intervals .
- **Enterprise** – Enterprise is more secure than WPA Personal. In this type, every client automatically receives a unique encryption key after securely logging on to the network. This key is automatically updated at regular intervals. WPA uses TKIP and WPA2 uses the AES algorithm.

Recommended Authentication and Encryption Combinations

The following table summarizes the recommendations for authentication and encryption combinations for the Wi-Fi networks.

Table 31: *Recommended Authentication and Encryption Combinations*

Network Type	Authentication	Encryption
Employee	802.1X	AES
Guest Network	Captive Portal	None
Voice Network or Handheld devices	802.1X or PSK as supported by the device	AES if possible, TKIP or WEP if necessary (combine with security settings assigned for a user role).

Support for Authentication Survivability

The authentication survivability feature supports a survivable authentication framework against the remote link failure when working with the external authentication servers. When enabled, this feature allows the W-IAPs to authenticate the previously connected clients against the cached credentials if the connection to the authentication server is temporarily lost.

Instant supports the following EAP standards for authentication survivability:

- **EAP-PEAP**: The Protected Extensible Authentication Protocol also known as Protected EAP or PEAP is a protocol that encapsulates EAP within a potentially encrypted and authenticated Transport Layer Security (TLS) tunnel. The EAP-PEAP supports the MSCHAPv2 and GTC methods.
- **EAP-TLS**: EAP-Transport Layer Security (EAP-TLS) is an IETF open standard that uses the Transport Layer Security (TLS) protocol.

When the authentication survivability feature is enabled, the following authentication process is used:

1. The client associates to a W-IAP and authenticates to the external authentication server. The external authentication server can be either CPPM (for EAP-PEAP) or RADIUS server (EAP-TLS).
2. Upon successful authentication, the associated W-IAP caches the authentication credentials of the connected users for the configured duration. The cache expiry duration for authentication survivability can be set within the range of 1-99 hours, with 24 hours being the default cache timeout duration.
3. If the client roams or tries to reconnect to the W-IAP and the remote link fails due to the unavailability of the authentication server, the W-IAP uses the cached credentials in the internal authentication server to authenticate the user. However, if the user tries to reconnect after the cache expiry, the authentication fails.
4. When the authentication server is available and if the client tries to reconnect, the W-IAP detects the availability of server and allows the client to authenticate to the server. Upon successful authentication, the W-IAP cache details are refreshed.

Configuring Authentication Survivability

You can enable authentication survivability for a wireless network profile through the UI or CLI.

In the Instant UI

To configure authentication survivability for a wireless network:

1. In the **Network** tab, click **New** to create a new network profile or select an existing profile for which you want to enable authentication survivability and click **edit**.
2. In the **Edit <profile-name>** or **New WLAN** window, ensure that all required WLAN and VLAN attributes are defined, and then click **Next**.
3. In the **Security** tab, under **Enterprise** security settings, select an existing authentication server or create a new server by clicking **New**.
4. To enable authentication survivability, select **Enabled** from the **Authentication survivability** drop-down. On enabling this, the W-IAP authenticates the previously connected clients using EAP-PEAP and EAP-TLS authentication when connection to the external authentication server is temporarily lost.
5. Specify the cache timeout duration, after which the cached details of the previously authenticated clients expire. You can specify a value within the range of 1-99 hours and the default cache timeout duration is 24 hours.
6. Click **Next** and then click **Finish** to apply the changes.

Important Points to Remember

- Any client connected through CPPM and authenticated through W-IAP remains authenticated with the W-IAP even if the client is removed from the CPPM server during the CPPM downtime.
- Do not make any changes to the authentication survivability cache timeout duration when the authentication server is down.
- For EAP-PEAP authentication, ensure that the CPPM 6.0.2 or later version is used for authentication. For EAP-TLS authentication, any external or third-party server can be used.
- For EAP-TLS authentication, ensure that the server and CA certificates from the authentication servers are uploaded on W-IAP. For more information, see Uploading Certificates on page 173.

In the CLI

To configure authentication survivability for a wireless network:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# type {<Employee> | <Voice>| <Guest>}
(Instant AP)(SSID Profile <name>)# auth-server <server-name1>
(Instant AP)(SSID Profile <name>)# auth-survivability
(Instant AP)(SSID Profile <name>)# exit
```

```
(Instant AP)(config)# auth-survivability cache-time-out <hours>
(Instant AP)(config)# end
(Instant AP)# commit apply
```

To view the cache expiry duration:

```
(Instant AP)# show auth-survivability time-out
```

To view the information cached by the W-IAP:

```
(Instant AP)# show auth-survivability cached-info
```

To view logs for debugging:

```
(Instant AP)# show auth-survivability debug-log
```

Configuring Authentication Servers

This section describes the following procedures:

- Configuring an External Server for Authentication on page 157
- Configuring Dynamic RADIUS Proxy Parameters on page 161

Configuring an External Server for Authentication

You can add an external RADIUS server, LDAP server, CPPM server for AirGroup or CoA through the Instant UI or CLI.

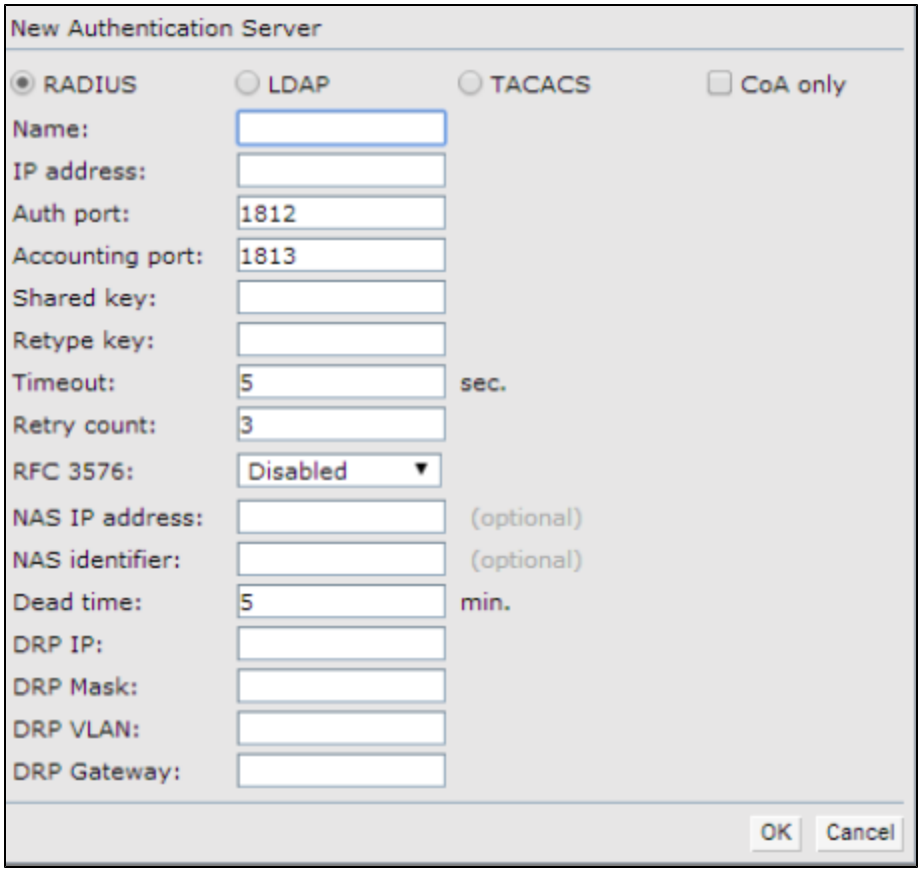
In 6.4.0.2-4.1 release, you can configure TACACS+ server for authenticating management users. For more information, on management users and TACACS+ server based authentication, see Configuring Authentication Parameters for Management Users ..

In the Instant UI

To configure an authentication server:

1. Navigate to **Security**>**Authentication Servers**. The **Security** window is displayed.
2. To create a new server, click **New**. A window for specifying details for the new server is displayed. The following figure shows the parameters to configure for a new RADIUS authentication server configuration:

Figure 46 *New Authentication Server Window*



3. Configure any of the following types of server:

- **RADIUS Server** – To configure a RADIUS server, specify the attributes described in the following table:

Table 32: *RADIUS Server Configuration Parameters*

Parameter	Description
Name	Enter the name of the new external RADIUS server.
IP address	Enter the IP address of the external RADIUS server.
Auth port	Enter the authorization port number of the external RADIUS server. The default port number is 1812.
Accounting port	Enter the accounting port number. This port is used for sending accounting records to the RADIUS server. The default port number is 1813.
Shared key	Enter a shared key for communicating with the external RADIUS server.
Retype key	Re-enter the shared key.
Timeout	Specify a timeout value in seconds. The value determines the timeout for one RADIUS request. The W-IAP retries to send the request several times (as configured in the **Retry count**), before the user gets disconnected. For example, if the **Timeout** is 5 seconds, **Retry counter** is 3, user is disconnected after 20 seconds. The default value is 5 seconds.

Parameter	Description
Retry count	Specify a number between 1 and 5. Indicates the maximum number of authentication requests that are sent to the server group, and the default value is 3 requests.
RFC 3576	Select **Enabled** to allow the APs to process RFC 3576-compliant Change of Authorization (CoA) and disconnect messages from the RADIUS server. Disconnect messages cause a user session to be terminated immediately, whereas the CoA messages modify session authorization attributes such as data filters.
NAS IP address	Enter the Virtual Controller IP address. The NAS IP address is the Virtual Controller IP address that is sent in data packets. **NOTE:** If you do not enter the IP address, the Virtual Controller IP address is used by default when **Dynamic RADIUS Proxy** is enabled.
NAS identifier	Use this to configure strings for RADIUS attribute 32, NAS Identifier, to be sent with RADIUS requests to the RADIUS server.
Dead Time	Specify a dead time for authentication server in minutes. When two or more authentication servers are configured on the W-IAP and a server is unavailable, the dead time configuration determines the duration for which the authentication server would be available if the server is marked as unavailable.
Dynamic RADIUS proxy parameters	Specify the following dynamic RADIUS proxy parameters: • **DRP IP**– IP address to be used as source IP for RADIUS packets • **DRP Mask**–Subnet mask of the DRP IP address. • **DRP VLAN**–VLAN in which the RADIUS packets are sent. • **DRP Gateway**–Gateway IP address of the DRP VLAN. For more information on dynamic RADIUS proxy parameters and configuration procedure, see Configuring Dynamic RADIUS Proxy Parameters on page 161.

- **LDAP Server** –To configure an LDAP server, select the **LDAP** option and specify the attributes described in the following table:

Table 33: *LDAP Server Configuration Parameters*

Parameter	Description
Name	Enter the name of the LDAP server.
IP address	Enter the IP address of the LDAP server.
Auth port	Enter the authorization port number of the LDAP server. The default port number is 389.
Admin-DN	Enter a distinguished name for the admin user with read/search privileges across all the entries in the LDAP database (the user need not have write privileges, but the user must be able to search the database, and read attributes of other users in the database).
Admin password	Enter a password for administrator.
Base-DN	Enter a distinguished name for the node that contains the entire user database.

Parameter	Description
Filter	Specify the filter to apply when searching for a user in the LDAP database. The default filter string is **(objectclass=*)**.
Key Attribute	Specify the attribute to use as a key while searching for the LDAP server. For Active Directory, the value is **sAMAccountName**
Timeout	Enter a value between 1 and 30 seconds. The default value is 5.
Retry count	Enter a value between 1 and 5. The default value is 3.
Dead Time	Specify a dead time for authentication server in minutes within the range of 1-1440 minutes. The default dead time interval is 5 minutes. When two or more authentication servers are configured on the W-IAP and a server is unavailable, the dead time configuration determines the duration for which the authentication server would be available if the server is marked as unavailable.

- **CPPM Server** for AirGroup CoA – To configure a CPPM server used for AirGroup CoA (Change of Authorization), select the **CoA only** checkbox. The RADIUS server is automatically selected.

Table 34: *CPPM Server Configuration Parameters for AirGroup CoA*

Parameter	Description
Name	Enter the name of the server.
IP address	Enter the IP address of the server.
Air Group CoA port	Enter a port number for sending AirGroup CoA on a different port than on the standard CoA port. The default value is 5999.
Shared key	Enter a shared key for communicating with the external RADIUS server.
Retype key	Re-enter the shared key.

4. Click **OK**.

The CPPM server acts as a RADIUS server and asynchronously provides the AirGroup parameters for the client device including shared user, role, and location.

To assign the RADIUS authentication server to a network profile, select the newly added server when configuring security settings for a wireless or wired network profile.

You can also add an external RADIUS server by selecting the **New** option when configuring a WLAN or wired profile. For more information, see Configuring Security Settings for a WLAN SSID Profile on page 99 and Configuring Security Settings for a Wired Profile on page 115.

In the CLI

To configure a RADIUS server:

```
(Instant AP)(config)# wlan auth-server <profile-name>
(Instant AP)(Auth Server <profile-name>)# ip <IP-address>
(Instant AP)(Auth Server <profile-name>)# key <key>
(Instant AP)(Auth Server <profile-name>)# port <port>
(Instant AP)(Auth Server <profile-name>)# acctport <port>
```

```
(Instant AP)(Auth Server <profile-name>)# nas-id <NAS-ID>
(Instant AP)(Auth Server <profile-name>)# nas-ip <NAS-IP-address>
(Instant AP)(Auth Server <profile-name>)# timeout <seconds>
(Instant AP)(Auth Server <profile-name>)# retry-count <number>
(Instant AP)(Auth Server <profile-name>)# rfc3576
(Instant AP)(Auth Server <profile-name>)# deadtime <minutes>
(Instant AP)(Auth Server <profile-name>)# drp-ip <IP-address> <mask> vlan <vlan> gateway
<gateway-IP-address)
(Instant AP)(Auth Server <profile-name>)# end
(Instant AP)# commit apply
(Instant AP)# commit apply
```

To configure an LDAP server:

```
(Instant AP)(config)# wlan ldap-server <profile-name>
(Instant AP)(LDAP Server <profile-name>)# ip <IP-address>
(Instant AP)(LDAP Server <profile-name>)# port <port>
(Instant AP)(LDAP Server <profile-name>)# admin-dn <name>
(Instant AP)(LDAP Server <profile-name>)# admin-password <password>
(Instant AP)(LDAP Server <profile-name>)# base-dn <name>
(Instant AP)(LDAP Server <profile-name>)# filter <filter>
(Instant AP)(LDAP Server <profile-name>)# key-attribute <key>
(Instant AP)(LDAP Server <profile-name>)# timeout <seconds>
(Instant AP)(LDAP Server <profile-name>)# retry-count <number>
(Instant AP)(LDAP Server <profile-name>)# deadtime <minutes>
(Instant AP)(LDAP Server <profile-name>)# end
(Instant AP)# commit apply
```

To configure a CPPM server used for AirGroup CoA (Change of Authorization):

```
(Instant AP)(config)# wlan auth-server <profile-name>
(Instant AP)(Auth Server <profile-name>)# ip <IP-address>
(Instant AP)(Auth Server <profile-name>)# key <key>
(Instant AP)(Auth Server <profile-name> # cppm-rfc3576-port <port>
(Instant AP)(Auth Server <profile-name>)# cppm-rfc3576-only
(Instant AP)(Auth Server <profile-name>)# end
(Instant AP)# commit apply
```

Configuring Dynamic RADIUS Proxy Parameters

The RADIUS server can be deployed at different locations and VLANs. In most cases, a centralized RADIUS or local server is used to authenticate users. However, some user networks can use a local RADIUS server for employee authentication and a centralized RADIUS based captive portal server for guest authentication. To ensure that the RADIUS traffic is routed to the required RADIUS server, the dynamic RADIUS proxy feature must be enabled.

If the W-IAP clients need to authenticate to the RADIUS servers through a different IP address and VLAN, ensure that the following steps are completed:

1. Enable dynamic RADIUS proxy.
2. Configure dynamic RADIUS proxy IP, VLAN. netmask, gateway for each authentication server.
3. Associate the authentication servers to SSID or a wired profile to which the clients connect.

After completing the above-mentioned configuration steps, you can authenticate the SSID users against the configured dynamic RADIUS proxy parameters.

Enabling Dynamic RADIUS Proxy

You can enable RADIUS Server Support using the Instant UI or CLI.

In the Instant UI

To enable RADIUS server support:

1. In the Instant main window, click the **System** link. The **System** window is displayed.
2. In the **General** tab of **System** window, select **Enabled** from the **Dynamic RADIUS Proxy** drop-down list.
3. Click **OK**.

When dynamic RADIUS proxy is enabled, ensure that a static Virtual Controller IP is configured. For more information on configuring Virtual Controller IP address, see Configuring Virtual Controller IP Address on page 76.

When dynamic RADIUS proxy is enabled, the Virtual Controller network uses the IP Address of the Virtual Controller for communication with external RADIUS servers. Ensure that the Virtual Controller IP Address is set as a NAS IP when configuring RADIUS server attributes with dynamic RADIUS proxy enabled. For more information on configuring RADIUS server attributes, see Configuring an External Server for Authentication on page 157.

In the CLI

To enable the dynamic RADIUS proxy feature:

```
(Instant AP)(config)# dynamic-radius-proxy
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Configuring Dynamic RADIUS Proxy Parameters for Authentication Servers

You can configure DRP parameters for the authentication server by using the Instant UI or CLI.

In the Instant UI

1. Click the **Security**>**Authentication Servers**.
2. To create a new server, click **New** and configure the required RADIUS server parameters as described in Table 32.
3. Ensure that the following dynamic RADIUS proxy parameters are configured:
   - **DRP IP**– IP address to be used as source IP for RADIUS packets
   - **DRP Mask**–Subnet mask of the DRP IP address.
   - **DRP VLAN**–VLAN in which the RADIUS packets are sent.
   - **DRP Gateway**–Gateway IP address of the DRP VLAN.
4. Click **OK**.

In the CLI

To configure dynamic RADIUS proxy parameters:

```
(Instant AP)(config)# wlan auth-server <profile-name>
(Instant AP)(Auth Server <profile-name>)# ip <IP-address>
(Instant AP)(Auth Server <profile-name>)# key <key>
(Instant AP)(Auth Server <profile-name>)# port <port>
(Instant AP)(Auth Server <profile-name>)# acctport <port>
(Instant AP)(Auth Server <profile-name>)# nas-id <NAS-ID>
(Instant AP)(Auth Server <profile-name>)# nas-ip <NAS-IP-address>
(Instant AP)(Auth Server <profile-name>)# timeout <seconds>
(Instant AP)(Auth Server <profile-name>)# retry-count <number>
(Instant AP)(Auth Server <profile-name>)# deadtime <minutes>
(Instant AP)(Auth Server <profile-name>)# drp-ip <IP-address> <mask> vlan <vlan> gateway
<gateway-IP-address>
(Instant AP)(Auth Server <profile-name>)# end
(Instant AP)# commit apply
```

Associate the Authentication Servers with an SSID or Wired Profile

1. Access the WLAN wizard or Wired Settings window.

- To open the WLAN wizard, select an existing SSID in the **Network** tab, and click **edit**.
- To open the wired settings window, click **More** > **Wired**. In the **Wired** window, select a profile and click **Edit**.

You can also associate the authentication servers when creating a new WLAN or wired profile.

2. Click the **Security** tab.
3. If you are configuring the authentication server for a WLAN SSID, under **Security** tab, slide to **Enterprise** security level.
4. Ensure that an authentication type is enabled.
5. From the **Authentication Server 1** drop-down list, select the server name on which dynamic RADIUS proxy parameters are enabled. You can also create a new server with RADIUS and RADIUS proxy parameters by selecting **New**.
6. Click **Next** and then click **Finish**.
7. To assign the RADIUS authentication server to a network profile, select the newly added server when configuring security settings for a wireless or wired network profile.

You can also add an external RADIUS server by selecting New for Authentication Server when configuring a WLAN or wired profile. For more information, see Configuring Security Settings for a WLAN SSID Profile on page 99 and Configuring Security Settings for a Wired Profile on page 115.

In the CLI

To associate an authentication server to a WLAN SSID:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name># auth-server <server-name>
(Instant AP)(SSID Profile <name># end
((Instant AP)# commit apply
```

To associate an authentication server to a wired profile:

```
(Instant AP)(config)# wired-port-profile <name>
(Instant AP)(wired ap profile <name>)# auth-server <name>
(Instant AP)(wired ap profile <name>)# end
(Instant AP)# commit apply
```

Configuring 802.1X Authentication for a Network Profile

The Instant network supports internal RADIUS server and external RADIUS server for 802.1X authentication.

The steps involved in 802.1X authentication are as follows:

1. The NAS requests authentication credentials from a wireless client.
2. The wireless client sends authentication credentials to the NAS.
3. The NAS sends these credentials to a RADIUS server.
4. The RADIUS server checks the user identity and authenticates the client if the user details are available in its database. The RADIUS server sends an *Access-Accept* message to the NAS. If the RADIUS server cannot identify the user, it stops the authentication process and sends an *Access-Reject* message to the NAS. The NAS forwards this message to the client and the client must re-authenticate with appropriate credentials.
5. After the client is authenticated, the RADIUS server forwards the encryption key to the NAS. The encryption key is used for encrypting or decrypting traffic sent to and from the client.

The NAS acts as a gateway to guard access to a protected resource. A client connecting to the wireless network first connects to the NAS.

Configuring 802.1X Authentication for a Wireless Network Profile

You can configure 802.1X authentication for a wireless network profile in the Instant UI or CLI.

In the Instant UI

To enable 802.1X authentication for a wireless network:

1. In the **Network** tab, click **New** to create a new network profile or select an existing profile for which you want to enable 802.1X authentication and click **edit**.
2. In the **Edit <profile-name>** or **New WLAN** window, ensure that all required WLAN and VLAN attributes are defined, and then click **Next**.
3. In the **Security** tab, specify the following parameters for the **Enterprise** security level:
   a. Select any of the following options from the **Key management** drop-down list.
      - WPA-2 Enterprise
      - WPA Enterprise
      - Both (WPA-2 & WPA)
      - Dynamic WEP with 802.1X
4. If you do not want to use a session key from the RADIUS Server to derive pair wise unicast keys, set **Session Key for LEAP** to **Enabled**.
5. To terminate the EAP portion of 802.1X authentication on the W-IAP instead of the RADIUS server, set **Termination** to **Enabled**.

   By default, for 802.1X authorization, the client conducts an EAP exchange with the RADIUS server, and the AP acts as a relay for this exchange. When **Termination** is enabled, the W-IAP by itself acts as an authentication server and terminates the outer layers of the EAP protocol, only relaying the innermost layer to the external RADIUS server.
6. Specify the type of authentication server to use and configure other required parameters. You can also configure two different authentication servers to function as primary and backup servers when termination is enabled. For more information on RADIUS authentication configuration parameters, see Configuring an External Server for Authentication on page 157.
7. Click **Next** to define access rules, and then click **Finish** to apply the changes.

In the CLI

To configure 802.1X authentication for a wireless network:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# type {<Employee>|<Voice>}
(Instant AP)(SSID Profile <name>)# opmode {wpa2-aes|wpa-tkip|wpa-tkip,wpa2-aes|dynamic-wep}
(Instant AP)(SSID Profile <name>)# leap-use-session-key
(Instant AP)(SSID Profile <name>)# termination
(Instant AP)(SSID Profile <name>)# auth-server <server1>
(Instant AP)(SSID Profile <name>)# auth-server <server2>
(Instant AP)(SSID Profile <name>)# radius-reauth-interval <minutes>
(Instant AP)(SSID Profile <name>)# auth-survivability
(Instant AP)(SSID Profile <name>)# exit
(Instant AP)(config)# auth-survivability cache-time-out <hours>
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Configuring 802.1X Authentication for Wired Profiles

You can configure 802.1X authentication for a wired profile in the Instant UI or CLI.

In the Instant UI

To enable 802.1X authentication for a wired profile:

1. Click the **Wired** link under **More** at the top right corner of the main window. The **Wired** window is displayed.
2. Click **New** under **Wired Networks** to create a new network or select an existing profile for which you want to enable 802.1X authentication and then click **Edit**.
3. In the **New Wired Network** or the **Edit Wired Network** window, ensure that all the required Wired and VLAN attributes are defined, and then click **Next**.
4. In the **Security** tab, select **Enabled** from the **802.1X authentication** drop-down list.
5. Specify the type of authentication server to use and configure other required parameters. For more information on configuration parameters, see Configuring Security Settings for a Wired Profile on page 115.
6. Click **Next** to define access rules, and then click **Finish** to apply the changes.
7. Assign the profile to an Ethernet port. For more information, see Assigning a Profile to Ethernet Ports on page 117.

In the CLI

To enable 802.1X authentication for a wired profile:

```
(Instant AP) (config)# wired-port-profile <name>
(Instant AP) (wired ap profile <name>)# type {<employee> |<guest>}
(Instant AP) (wired ap profile <name>)# dot1x
(Instant AP) (wired ap profile <name>)# auth-server <server1>
(Instant AP) (wired ap profile <name>)# auth-server <server2>
(Instant AP) (wired ap profile <name>)# server-load-balancing
(Instant AP) (wired ap profile <name>)# radius-reauth-interval <Minutes>
(Instant AP) (wired ap profile <name>)# end
(Instant AP)# commit apply
```

Configuring MAC Authentication for a Network Profile

MAC authentication can be used alone or it can be combined with other forms of authentication such as WEP authentication. However, it is recommended that you do not use the MAC-based authentication.

This section describes the following procedures:

- Configuring MAC Authentication for Wireless Network Profiles on page 165
- Configuring MAC Authentication for Wired Profiles on page 166

Configuring MAC Authentication for Wireless Network Profiles

You can configure MAC authentication for a wired profile in the Instant UI or CLI.

In the Instant UI

To enable MAC Authentication for a wireless network:

1. In the **Network** tab, click **New** to create a new network profile or select an existing profile for which you want to enable MAC authentication and click **edit**.
2. In the **Edit <profile-name>** or **New WLAN** window, ensure that all required WLAN and VLAN attributes are defined, and then click **Next**.
3. In the **Security** tab, select **Enabled** from the **MAC authentication** drop-down list, for **Personal** or **Open** security level.
4. Specify the type of authentication server to use.

5. If the internal authentication server is used, perform the following steps to allow MAC address based authentication:
   a. Click the **Users** link against the **Internal server** field. The **Users** window is displayed.
   b. Specify the client MAC address as the user name and password.
   c. Specify the type of the user (employee or guest).
   d. Click **Add**.
   e. Repeat the steps to add more users.
   f. Click **OK**.
6. To allow the W-IAP to use a delimiter in the MAC authentication request, specify a character (for example, colon or dash) as a delimiter for the MAC address string. For example, if you specify the colon as a delimiter, MAC addresses in the xx:xx:xx:xx:xx:xx format are used. If the delimiter is not specified, the MAC address in the xxxxxxxxxxxx format is used.
7. To allow the W-IAP to use uppercase letters in the MAC address string, set **Uppercase support** to **Enabled**.
8. Configure other parameters as required.
9. Click **Next** to define access rules, and then click **Finish** to apply the changes.

In the CLI

To configure MAC-address based authentication with external server:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# type {<Employee> | <Voice>| <Guest>}
(Instant AP)(SSID Profile <name>)# mac-authentication
(Instant AP)(SSID Profile <name>)# mac-authentication-delimiter <delim>
(Instant AP)(SSID Profile <name>)# mac-authentication-upper-case
(Instant AP)(SSID Profile <name>)# external-server
(Instant AP)(SSID Profile <name>)# auth-server <server-name1>
(Instant AP)(SSID Profile <name>)# auth-server <server-name2>
(Instant AP)(SSID Profile <name>)# server-load-balancing
(Instant AP)(SSID Profile <name>)# radius-reauth-interval <minutes>
(Instant AP)(SSID Profile <name>)# end
(Instant AP)# commit apply
```

To add users for MAC authentication based on internal authentication server:

```
(Instant AP)(config)# user <username> [<password>] [portal| radius]
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Configuring MAC Authentication for Wired Profiles

You can configure MAC authentication for a wired profile in the Instant UI or CLI.

In the Instant UI

To enable MAC authentication for a wired profile:

1. Click the **Wired** link under **More** at the top right corner of the main window. The **Wired** window is displayed.
2. Click **New** under **Wired Networks** to create a new network or select an existing profile for which you want to enable MAC authentication and then click **Edit**.
3. In the **New Wired Network** or the **Edit Wired Network** window, ensure that all the required Wired and VLAN attributes are defined, and then click **Next**.
4. In the **Security** tab, select **Enabled** from the **MAC authentication** drop-down list.
5. Specify the type of authentication server to use.

6. If the internal authentication server is used, perform the following steps to allow MAC address based authentication:
   a. Click the **Users** link against the **Internal server** field. The **Users** window is displayed.
   b. Specify the client MAC address as the user name and password.
   c. Specify the type of the user (employee or guest).
   d. Click **Add**.
   e. Repeat the steps to add more users.
   f. Click **OK**.
7. Configure other parameters as required.
8. Click **Next** to define access rules, and then click **Finish** to apply the changes.

In the CLI

To configure MAC-address based authentication with external server:

```
(Instant AP)(config)# wired-port-profile <name>
(Instant AP)(wired ap profile <name>)# type {<employee> |<guest>}
(Instant AP)(wired ap profile <name>)# mac-authentication
(Instant AP)(wired ap profile <name>)# auth-server <server-1>
(Instant AP)(wired ap profile <name>)# auth-server <server-2>
(Instant AP)(wired ap profile <name>)# server-load-balancing
(Instant AP)(wired ap profile <name>)# radius-reauth-interval <Minutes>
(Instant AP)(wired ap profile <name>)# end
(Instant AP)# commit apply
```

To add users for MAC authentication based on internal authentication server:

```
(Instant AP)(config)# user <username> [<password>] [portal| radius]
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Configuring MAC Authentication with 802.1X Authentication

This section describes the following procedures:

- Configuring MAC and 802.1X Authentication for a Wireless Network Profile on page 167
- Configuring MAC and 802.1X Authentication for Wired Profiles on page 168

Configuring MAC and 802.1X Authentication for a Wireless Network Profile

You can configure MAC authentication with 802.1X authentication for wireless network profile using the Instant UI or CLI.

In the Instant UI

To configure both MAC and 802.1X authentication for a wireless network:

1. In the **Network** tab, click **New** to create a new network profile or select an existing profile for which you want to enable MAC and 802.1X authentication and click **edit**.
2. In the **Edit <profile-name>** or **New WLAN** window, ensure that all required WLAN and VLAN attributes are defined, and then click **Next**.
3. In the **Security** tab, ensure that the required parameters for MAC authentication and 802.1X authentication are configured.
4. Select the **Perform MAC authentication before 802.1X** checkbox to use 802.1X authentication only when the MAC authentication is successful.

5. Select the checkbox **MAC authentication fail-thru** to use 802.1X authentication even when the MAC authentication fails.
6. Click **Next** and then click **Finish** to apply the changes.

In the CLI

To configure both MAC and 802.1X authentication for a wireless network:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# type {<Employee> | <Voice>| <Guest>}
(Instant AP)(SSID Profile <name>)# mac-authentication
(Instant AP)(SSID Profile <name>)# l2-auth-failthrough
(Instant AP)(SSID Profile <name>)# auth-server <server-name1>
(Instant AP)(SSID Profile <name>)# radius-reauth-interval <minutes>
(Instant AP)(SSID Profile <name>)# auth-survivability
(Instant AP)(SSID Profile <name>)# exit
(Instant AP)(config)# auth-survivability cache-time-out <hours>
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Configuring MAC and 802.1X Authentication for Wired Profiles

You can configure MAC and 802.1X authentication for a wired profile in the Instant UI or CLI.

In the Instant UI

To enable MAC and 802.1X authentication for a wired profile:

1. Click the **Wired** link under **More** at the top right corner of the main window. The **Wired** window is displayed.
2. Click **New** under **Wired Networks** to create a new network or select an existing profile for which you want to enable MAC authentication and then click **Edit**.
3. In the **New Wired Network** or the **Edit Wired Network** window, ensure that all the required Wired and VLAN attributes are defined, and then click **Next**.
4. In the **Security** tab, enable the following options:
   - Select **Enabled** from the **MAC authentication** drop-down list.
   - Select **Enabled** from the **802.1X authentication** drop-down list.
   - Select **Enabled** from the **MAC authentication fail-thru** drop-down list.
5. Specify the type of authentication server to use and configure other required parameters. For more information on configuration parameters, see Configuring Security Settings for a Wired Profile on page 115
6. Click **Next** to define access rules, and then click **Finish** to apply the changes.

In the CLI

To enable MAC and 802.1X authentication for a wired profile:

```
(Instant AP)(config)# wired-port-profile <name>
(Instant AP)(wired ap profile "<name>")# type {<employee> |<guest>}
(Instant AP)(wired ap profile "<name>")# mac-authentication
(Instant AP)(wired ap profile "<name>")# dot1x
(Instant AP)(wired ap profile "<name>")# l2-auth-failthrough
(Instant AP)(wired ap profile "<name>")# auth-server <name>
(Instant AP)(wired ap profile "<name>")# server-load-balancing
(Instant AP)(wired ap profile "<name>")# radius-reauth-interval <Minutes>
(Instant AP)(wired ap profile "<name>")# end
(Instant AP)# commit apply
```

Configuring MAC Authentication with Captive Portal Authentication

This authentication method has the following features:

- If the captive portal splash page type is **Internal-Authenticated** or **External-RADIUS Server**, MAC authentication reuses the server configurations.
- If the captive portal splash page type is **Internal-Acknowledged** or **External-Authentication Text** and MAC authentication is enabled, a server configuration page is displayed.
- If the captive portal splash page type is **none**, MAC authentication is disabled.
- MAC authentication only role– You can use the WLAN wizard to configure the **mac-auth-only** role in the role-based access rule configuration section when MAC authentication is enabled with captive portal authentication.

Configuring MAC Authentication with Captive Portal Authentication

You can configure the MAC authentication with Captive Portal authentication for a network profile using the Instant UI or CLI.

In the Instant UI

1. Select an existing wireless or wired profile for which you want to enable MAC with Captive Portal authentication. Depending on the network profile selected, the **Edit <WLAN-Profile>** or **Edit Wired Network** window is displayed.

You can configure MAC authentication with Captive Portal authentication, in the **Access** tab of the **New WLAN** and **New Wired Network** windows when configuring a new profile.

2. In the **Access** tab, specify the following parameters for a network with **Role-Based** rules:
   a. Select the **Enforce Machine Authentication** checkbox when MAC authentication is enabled for Captive Portal. If the MAC authentication fails, the Captive Portal authentication role is assigned to the client.
   b. For wireless network profile, select **Enforce MAC Auth Only Role** checkbox when MAC authentication is enabled for Captive Portal. After successful MAC authentication, MAC auth only role is assigned to the client.
3. Click **Next** and then click **Finish** to apply the changes.

In the CLI

To configure MAC authentication with Captive Portal authentication for a wireless profile:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# type <Guest>
(Instant AP)(SSID Profile <name>)# mac-authentication
(Instant AP)(SSID Profile <name>)# captive-portal <type> exclude-uplink <type>
(Instant AP)(SSID Profile <name>)# set-role-machine-auth <machine-authentication> <user-
authentication>
(Instant AP)(SSID Profile <name>)# set-role-mac-auth <MAC-authentication-only>
(Instant AP)(SSID Profile <name>)# end
(Instant AP)# commit apply
```

To configure MAC authentication with Captive Portal authentication for a wired profile:

```
(Instant AP)(config)# wired-port-profile <name>
(Instant AP)(wired ap profile <name>)# type <guest>
(Instant AP)(wired ap profile <name>)# mac-authentication
(Instant AP)(wired ap profile <name>)# captive-portal <type>
(Instant AP)(wired ap profile <name>)# captive-portal <type> exclude-uplink {<3G>| <4G>|
<Wifi> | Ethernet}
(Instant AP)(wired ap profile <name>)# set-role-machine-auth <machine-only> <user-only>
(Instant AP)(wired ap profile <name>)# set-role-mac-auth <mac-only>
(Instant AP)(wired ap profile <name>)# end
```

```
(Instant AP)# commit apply
```

Configuring WISPr Authentication

Instant supports the following smart clients:

- iPass
- Boingo

These smart clients enable client authentication and roaming between hotspots by embedding iPass Generic Interface Specification (GIS) *redirect*, *authentication*, and *logoff* messages within HTML messages that are sent to the W-IAP.

NOTE

WISPr authentication is supported only for the **Internal - Authenticated** and **External - RADIUS Server** captive portal authentication. Select the **Internal - Authenticated** or the **External - RADIUS Server** option from the **Splash page type** drop-down list to configure WISPr authentication for a WLAN profile.

You can configure WISPr authentication using the Instant UI or CLI.

In the Instant UI

1. Click the **System** link at the top-right corner of the Instant main window. The **System** window is displayed.
2. Click **Show advanced options**.
3. Click **WISPr** tab. The **WISPr** tab contents are displayed. The following figure shows the **WISPr** tab contents:

Figure 47 *Configuring WISPr Authentication*

4. Enter the ISO Country Code for the WISPr Location ID in the **ISO Country Code** text box.
5. Enter the E.164 Area Code for the WISPr Location ID in the **E.164 Area Code** text box.
6. Enter the operator name of the Hotspot in the **Operator Name** text box.
7. Enter the E.164 Country Code for the WISPr Location ID in the **E.164 Country Code** text box.
8. Enter the SSID/Zone section for the WISPr Location ID in the **SSID/Zone** text box.
9. Enter the name of the Hotspot location in the **Location Name** text box. If no name is defined, the name of the W-IAP to which the user is associated is used.
10. Click **OK** to apply the changes.

The WISPr RADIUS attributes and configuration parameters are specific to the RADIUS server used by your ISP for the WISPr authentication. Contact your ISP to determine these values. You can find a list of ISO and ITU country and area codes at the ISO and ITU websites (**iso.org** and **itu.int**).

NOTE

A Boingo smart client uses a NAS identifier in the format <CarrierID>_<VenueID> for location identification. To support Boingo clients, ensure that you configure the NAS identifier parameter in the Radius server profile for the WISPr server.

In the CLI

```
(Instant AP)(config)# wlan wispr-profile
```

```
(Instant AP)(WISPr)# wispr-location-id-ac
(Instant AP)(WISPr)# wispr-location-id-cc
(Instant AP)(WISPr)# wispr-location-id-isocc
(Instant AP)(WISPr)# wispr-location-id-network
(Instant AP)(WISPr)# wispr-location-name-location
(Instant AP)(WISPr)# wispr-location-name-operator-name
(Instant AP)(WISPr)# end
(Instant AP)# commit apply
```

Blacklisting Clients

The client blacklisting denies connection to the blacklisted clients. When a client is blacklisted, it is not allowed to associate with a W-IAP in the network. If a client is connected to the network when it is blacklisted, a deauthentication message is sent to force client disconnection.

This section describes the following procedures:

- Blacklisting Clients Manually on page 171
- Blacklisting Users Dynamically on page 172

Blacklisting Clients Manually

Manual blacklisting adds the MAC address of a client to the blacklist. These clients are added into a permanent blacklist. These clients are not allowed to connect to the network unless they are removed from the blacklist.

Adding a Client to the Blacklist

You can add a client to the blacklist manually using the Instant UI or CLI.

In the Instant UI

1. Click the **Security** link from the top right corner of the Instant main window.
2. Click the **Blacklisting** tab.
3. Under the **Manual Blacklisting**, click **New**.
4. Enter the MAC address of the client to be blacklisted in the **MAC address to add** text box.
5. Click **OK**. The **Blacklisted Since** tab displays the time at which the current blacklisting has started for the client.
6. To delete a client from the manual blacklist, select the MAC Address of the client under the **Manual Blacklisting**, and then click **Delete**.

In the CLI

To blacklist a client:

```
(Instant AP)(config)# blacklist-client <MAC-Address>
(Instant AP)(config)# end
(Instant AP)# commit apply
```

To view the blacklisted clients:

```
(Instant AP)# show blacklist-client

Blacklisted Clients
-------------------
MAC Reason Timestamp Remaining time(sec) AP name
--- ------ --------- ------------------ -------
00:1c:b3:09:85:15 user-defined 17:21:29 Permanent -
```

Blacklisting Users Dynamically

The clients can be blacklisted dynamically when they exceed the authentication failure threshold or when a blacklisting rule is triggered as part of the authentication process.

Authentication Failure Blacklisting

When a client takes time to authenticate and exceeds the configured failure threshold, it is automatically blacklisted by a W-IAP.

Session Firewall Based Blacklisting

In session firewall based blacklisting, an ACL rule is used to enable the option for automation blacklisting. When the ACL rule is triggered, it sends out blacklist information and the client is blacklisted.

Configuring Blacklist Duration

You can set the blacklist duration using the Instant UI or CLI.

In the Instant UI

To set a blacklist duration:

1. Click the **Security** link from the top right corner of the Instant main window.
2. Click the **Blacklisting** tab.
3. Under Dynamic Blacklisting:
4. For **Auth failure blacklist time**, the duration in seconds after which the clients that exceed the authentication failure threshold must be blacklisted.
5. For **PEF rule blacklisted time**, enter the duration in seconds after which the clients can be blacklisted due to an ACL rule trigger.

You can configure a maximum number of authentication failures by the clients, after which a client must be blacklisted. For more information on configuring maximum authentication failure attempts, see Configuring Security Settings for a WLAN SSID Profile on page 99

To enable session firewall based blacklisting, click **New** and navigate to **WLAN Settings > VLAN > Security > Access** window, and enable the **Blacklist** option of the corresponding ACL rule.

In the CLI

To dynamically blacklist clients:

```
(Instant AP)(config)# auth-failure-blacklist-time <seconds>
(Instant AP)(config)# blacklist-time <seconds>
(Instant AP)(config)# end
(Instant AP)# commit apply
```

To view the blacklisted clients:

```
(Instant AP)# show blacklist-client config

Blacklist Time :60
Auth Failure Blacklist Time :60
Manually Blacklisted Clients
----------------------------
MAC Time
--- ----
Dynamically Blacklisted Clients
-------------------------------
MAC Reason Timestamp Remaining time(sec) AP IP
--- ------ --------- ------------------ -----
Dyn Blacklist Count :0
```

Uploading Certificates

A certificate is a digital file that certifies the identity of the organization or products of the organization. It is also used to establish your credentials for any Web transactions. It contains the organization name, a serial number, expiration date, a copy of the certificate-holder's public key, and the digital signature of the certificate-issuing authority so that a recipient can ensure that the certificate is real.

Instant supports the following certificate files:

- Auth server or captive portal server certificate: PEM format with passphrase (PSK)
- CA certificate: PEM or DER format

In the current release, W-IAP supports uploading of a customized certificate for internal captive portal server.

This section describes the following procedures:

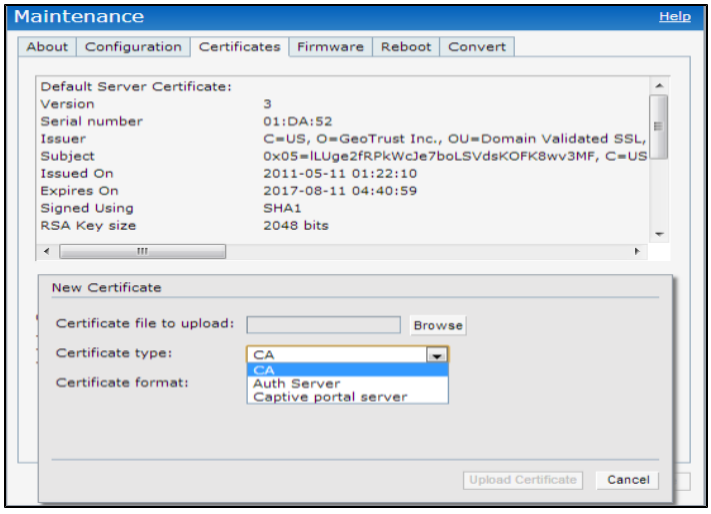
- Loading Certificates through Instant UI on page 173
- Loading Certificates through Instant CLI
- Loading Certificates through W-AirWave on page 174

Loading Certificates through Instant UI

To load a certificate in the Instant UI:

1. Click the **Maintenance** link at the top right corner of the Instant main window.
2. Click the **Certificates** tab. The **Certificates** tab contents are displayed. The following figure shows the **Certificates** window:

Figure 48 *Maintenance Window: Certificates Tab*



3. To upload a certificate, click **Upload New Certificate**. The **New Certificate** window is displayed.
4. Browse and select the file to upload.
5. Select any of the following types of certificates from the **Certificate type** drop-down list:

- CA–CA certificates validate the client's certificate.
- Auth Server–The authentication server certificate verifies the server's identity to the client.
- Captive portal server–Captive portal server certificate verifies internal captive portal server's identity to the client.

6. Select the certificate format from the **Certificate format** drop-down list.
7. If you have selected **Auth Server** or **Captive portal server** type, enter a passphrase in **Passphrase** and reconfirm. The default password is **whatever**. If the certificate does not include a passphrase, there is no passphrase required.

8. Click **Browse** and select the appropriate certificate file, and click **Upload Certificate**. The **Certificate Successfully Installed** message is displayed.

Loading Certificates through Instant CLI

To upload a certificate:

```
(Instant AP)# copy tftp {<ip-address> <filename> cpserver cert <password> format {p12|pem}
|system {1xca [format {der|pem}]|1xcert <passsword>[format {p12|pem}]}
```

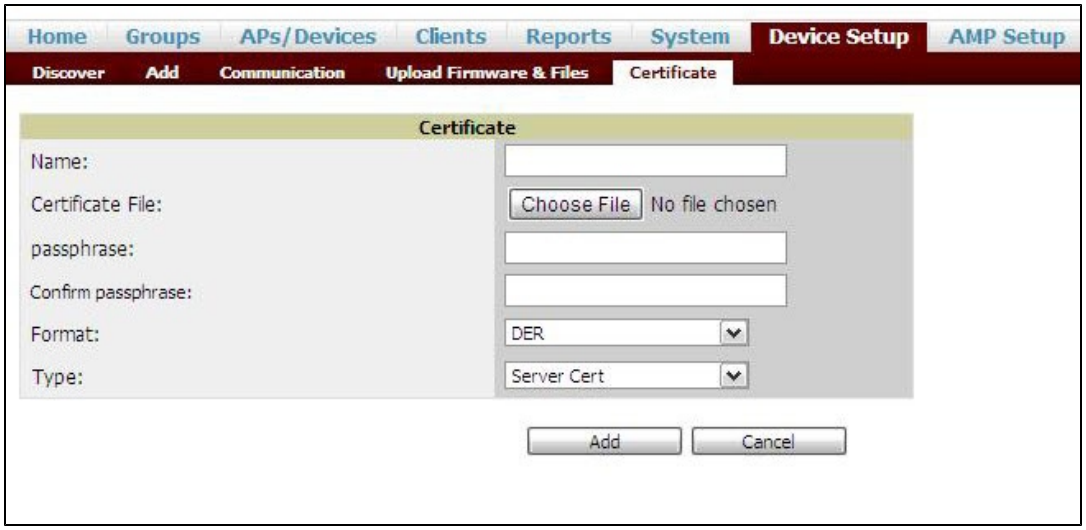
Loading Certificates through W-AirWave

You can manage certificates using the W-AirWave. The AMP directly provisions the certificates and performs basic certificate verification (such as certificate type, format, version, serial number and so on), before accepting the certificate and uploading to a W-IAP network. The AMP packages the text of the certificate into an HTTPS message and sends it to the Virtual Controller. After the VC receives this message, it draws the certificate content from the message, converts it to the right format, and saves it on the RADIUS server.

To load a certificate in W-AirWave:

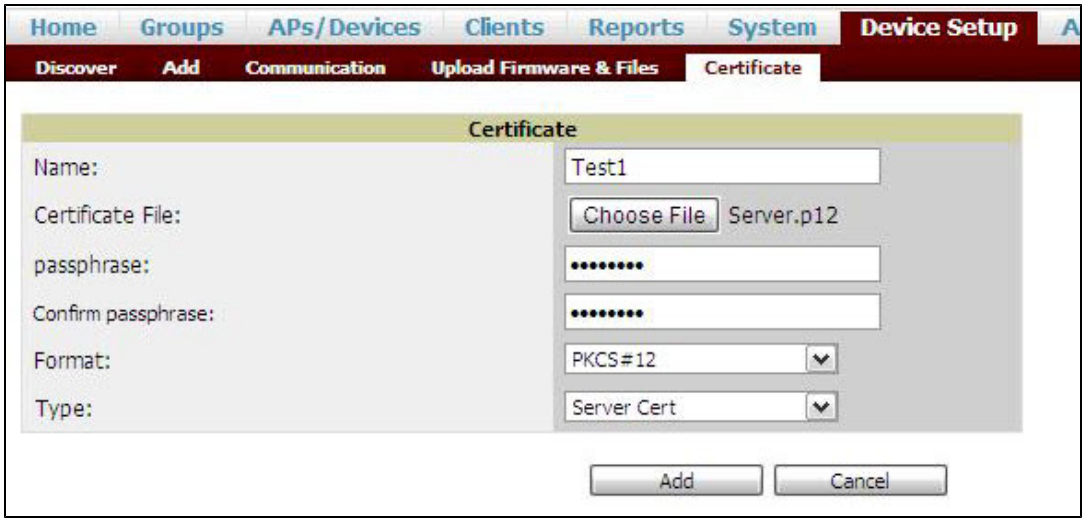
1. Navigate to **Device Setup > Certificate** and then click **Add** to add a new certificate. The **Certificate** window is displayed.
2. Enter the certificate **Name**, and click **Choose File** to browse and upload the certificate.

Figure 49 *Loading Certificate via W-AirWave*



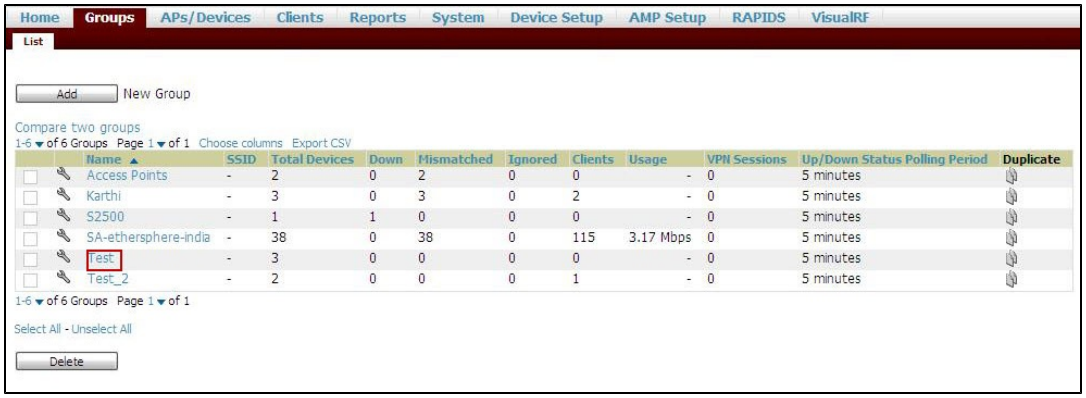
3. Select the appropriate **Format** that matches the certificate file name. Select **Server Cert** for certificate **Type**, and provide the passphrase if you want to upload a Server certificate. Select either **Intermediate CA** or **Trusted CA** certificate **Type**, if you want to upload a CA certificate.

Figure 50 *Server Certificate*



4. After you upload the certificate, navigate to **Groups,** click the Instant **Group** and then select **Basic**. The Group name is displayed only if you have entered the **Organization** name in the Instant UI. For more information, see Configuring Organization String on page 277 for further information.

Figure 51 *Selecting the Group*



The **Virtual Controller Certificate** section displays the certificates (CA cert and Server).

5. Click **Save** to apply the changes only to W-AirWave. Click **Save and Apply** to apply the changes to the W-IAP.
6. To clear the certificate options, click **Revert**.

This chapter describes the procedures for configuring user roles, role assignment, and firewall policies.

- Firewall Policies on page 176
- Content Filtering on page 186
- Configuring User Roles on page 190
- Configuring Derivation Rules on page 192

Firewall Policies

Instant firewall provides identity-based controls to enforce application-layer security, prioritization, traffic forwarding, and network performance policies for wired and wireless networks. Using Instant firewall, you can enforce network access policies that define access to the network, areas of the network that users may access, and the performance thresholds of various applications.

Instant supports a role-based stateful firewall. Instant firewall recognizes flows in a network and keeps track of the state of sessions. Instant firewall manages packets according to the first rule that matches packet. The firewall logs on the W-IAPs are generated as syslog messages.

Access Control List Rules

You can use Access Control List (ACL) rules to either permit or deny data packets passing through the W-IAP. You can also limit packets or bandwidth available to a set of user roles by defining access rules. By adding custom rules, you can block or allow access based on the service or application, source or destination IP addresses.

You can create access rules to allow or block data packets that match the criteria defined in an access rule. You can create rules for either inbound traffic or outbound traffic. Inbound rules explicitly allow or block the inbound network traffic that matches the criteria in the rule. Outbound rules explicitly allow or block the network traffic that matches the criteria in the rule. For example, you can configure a rule to explicitly block outbound traffic to an IP address through the firewall.

The W-IAP clients are associated with user roles, which determine the client's network privileges and the frequency at which clients re-authenticate.

Instant supports the following types of ACLs:

- ACLs that permit or deny traffic based on the source IP address of the packet.
- ACLs that permit or deny traffic based on source or destination IP address, source or destination port number.
- ACLs that permit or deny traffic based on network services, application, application categories, web categories, and security ratings.

You can configure up to 128 access control entries in an ACL for a user role.

For more information on configuring firewall rules, see:

- Configuring Access Rules for Network Services on page 177.
- Configuring Network Address Translation Rules on page 179
- Configuring Inbound Firewall Rules on page 183
- Configuring Access Rules for Application and Application Categories on page 246

- Configuring Web Policy Enforcement on page 249

Configuring Access Rules for Network Services

This section describes the procedure for configuring ACLs to control access to network services. For information on:

- Configuring access rules based on application and application categories, see Configuring Access Rules for Application and Application Categories on page 246.
- Configuring access rules based on web categories and web reputation, see Configuring Web Policy Enforcement on page 249.

In the Instant UI

To configure ACL rules for a user role:

1. Navigate to **Security** > **Roles** tab. The **Roles** tab contents are displayed.

   You can also configure access rules for a wired or wireless client through the WLAN wizard (**Network** tab>**WLAN SSID**> **Edit**>**Edit WLAN** > **Access**) or the Wired profile (**More** > **Wired**>**Edit**> **Edit Wired Network**> **Access**) window.
2. Select the role for which you want to configure access rules.
3. In **Access rules** section, click **New** to add a new rule. The **New Rule** window is displayed.
4. Ensure that the rule type is set to **Access Control**
5. To configure a rule to control access to network services, select **Network** under service category and specify the following parameters:

Table 35: *Access Rule Configuration Parameters*

Service Category	Description
Network	Select a service from the list of available services. You can allow or deny access to any or all of the following services based on your requirement: • **any**–Access is allowed or denied to all services. • **custom**–Available options are TCP, UDP, and Other. If you select the TCP or UDP options, enter appropriate port numbers. If you select the Other option, enter the appropriate ID. **NOTE:** If TCP and UDP uses the same port, ensure that you configure separate access rules to permit or deny access.
Action	Select any of following actions: • Select **Allow** to allow access users based on the access rule. • Select **Deny** to deny access to users based on the access rule. • Select **Destination-NAT** to allow changes to destination IP address. • Select **Source-NAT** to allow changes to the source IP address. The destination-nat and source-nat actions apply only to the network services rules.
Destination	Select a destination option for the access rules for network services, applications, and application categories. You can allow or deny access to any the following destinations based on your requirements. • **to all destinations**– Access is allowed or denied to all destinations. • **to a particular server**–Access is allowed or denied to a particular server. After selecting this option, specify the IP address of the destination server. • **except to a particular server**–Access is allowed or denied to servers other than the specified server. After selecting this option, specify the IP address of the destination server. • **to a network**–Access is allowed or denied to a network. After selecting this option, specify

Table 35: *Access Rule Configuration Parameters*

Service Category	Description
	the IP address and netmask for the destination network. • **except to a network**–Access is allowed or denied to networks other than the specified network. After selecting this option, specify the IP address and netmask of the destination network. • **to domain name**–Access is allowed or denied to the specified domains. After selecting this option, specify the domain name in the **Domain Name** text box.
Log	Select this checkbox if you want a log entry to be created when this rule is triggered. Instant supports firewall based logging function. Firewall logs on the W-IAPs are generated as security logs.
Blacklist	Select the **Blacklist** checkbox to blacklist the client when this rule is triggered. The blacklisting lasts for the duration specified as **Auth failure blacklist time** on the Blacklisting tab of the **Security** window. For more information, see Blacklisting Clients on page 171.
Classify media	Select the **Classify media** checkbox to prioritize video and voice traffic. When enabled, a packet inspection is performed on all non-NAT traffic and the traffic is marked as follows: • Video: Priority 5 (Critical) • Voice: Priority 6 (Internetwork Control)
Disable scanning	Select **Disable scanning** checkbox to disable ARM scanning when this rule is triggered. The selection of the **Disable scanning** applies only if ARM scanning is enabled, For more information, see Configuring Radio Settings for a W-IAP on page 238.
DSCP tag	Select the **DSCP tag** checkbox to specify a DSCP value to prioritize traffic when this rule is triggered. Specify a value within the range of 0 to 63. To assign a higher priority, specify a higher value.
802.1p priority	Select the **802.1p priority** checkbox to specify an 802.1p priority. Specify a value between 0 and 7. To assign a higher priority, specify a higher value.

6. Click **OK** and then click **Finish**.

In the CLI

To configure access rules:

```
(Instant AP)(config)# wlan access-rule <access-rule-name>
(Instant AP)(Access Rule <Name>)#rule <dest> <mask> <match/invert> {<protocol> <start-port>
<end-port> {permit|deny|src-nat|dst-nat{<IP-address> <port>| <port>}}[<option1....option9>]
(Instant AP)(Access Rule <Name>)# end
(Instant AP)# commit apply
```

Example

```
(Instant AP)(config)# wlan access-rule employee
(Instant AP)(Access Rule "employee")# rule 10.17.88.59 255.255.255.255 match 6 4343 4343 log
classify-media
(Instant AP)(Access Rule "employee")# rule 192.0.2.8 255.255.255.255 invert 6 110 110 permit
(Instant AP)(Access Rule "employee")# rule 192.0.2.2 255.255.255.0 192.0.2.7 255.255.255.0
match tcp 21 21 deny
(Instant AP)(Access Rule "employee")# rule 192.0.2.2 255.255.255.0 192.0.2.7 255.255.255.0
match udp 21 21 deny
(Instant AP)(Access Rule "employee")# rule 192.0.2.2 255.255.255.0 match 6 631 631 permit
(Instant AP)(Access Rule "employee")# rule 192.0.2.8 255.255.255.255 invert 6 21 21 deny
(Instant AP)(Access Rule "employee")# rule 192.0.2.1 255.255.255.0 invert 17 67 69 deny
(Instant AP)(Access Rule "employee")# end
(Instant AP)# commit apply
```

Configuring Network Address Translation Rules

Network Address Translation (NAT) is the process of modifying network address information when packets pass through a routing device. The routing device acts as an agent between the public (the Internet) and private (local network), which allows translation of private network IP addresses to a public address space.

Instant supports the NAT mechanism to allow a routing device to use the translation tables to map the private addresses into a single IP address and packets are sent from this address, so that they appear to originate from the routing device. Similarly, if the packets are sent to the private IP address, the destination address is translated as per the information stored in the translation tables of the routing device.

Configuring a Source NAT Access Rule

The source NAT action in access rules allows the user to override the routing profile entries. For example, when a routing profile is configured to use 0.0.0.0/0, the client traffic in L3 mode access on an SSID destined to the corporate network is sent to the tunnel. When an access rule is configured with **Source NAT** action, the users can specify the service, protocol, or destination to which the source NAT is applied.

You can also configure source based routing to allow client traffic on one SSID to reach the Internet through the corporate network, while the other SSID can be used as an alternate uplink. You can create an access rule to perform source NAT by using the Instant UI or CLI.

In the Instant UI

To configure a source NAT access rule:

1. Navigate to the WLAN wizard or Wired settings window:
   - To configure access rules for a WLAN SSID, in the **Network** tab, click **New** to create a new network profile or **edit** to modify an existing profile.
   - To configure access rules for a wired profile, **More** > **Wired**. In the **Wired** window, click **New** under **Wired Networks** to create a new network or click **Edit** to select an existing profile.
2. Click the **Access** tab.
3. To configure access rules for the network, slide to **Network-based**. To configure access rules for user roles, slide to **Role-based**.
4. To create a new rule for the network, click **New**. To create an access rule for a user role, select the user role and then click **New**. The **New Rule** window is displayed.
5. In the **New Rule** window:
6. Select **Access control** from the **Rule type** drop-down list.
7. Select **Source-NAT** from the **Action** drop-down list, to allow changes to the source IP address.
8. Select a service from the list of available services.
9. Select the required option from the **Destination** drop-down list.
10. If required, enable other parameters such as **Log**, **Blacklist**, **Classify media**, **Disable scanning**, **DSCP tag**, and **802.1p priority**.
11. Click **OK** and then click **Finish**.

In the CLI

To configure source NAT access rule:

```
(Instant AP)(config)# wlan access-rule <access_rule>
(Instant AP)(Access Rule "<access_rule>")# rule <dest> <mask> <match> <protocol> <sport>
<eport> src-nat
(Instant AP)(Access Rule "<access_rule>")# end
(Instant AP)# commit apply
```

Configuring Source-Based Routing

To allow different forwarding policies for different SSIDs, you can configure source-based routing. The source-based routing configuration overrides the routing profile configuration and allows any destination or service to be configured to have direct access to the Internet (bypassing VPN tunnel) based on the ACL rule definition. When source-based routing is enabled, the Virtual Controller performs source NAT by using its uplink IP address.

To configure source-based routing:

1. Ensure that an L3 subnet with the netmask, gateway, VLAN, and IP address is configured. For more information on configuring L3 subnet, see Configuring L3-Mobility on page 307.
2. Ensure that the source IP address is associated with the IP address configured for the L3 subnet.
3. Create an access rule for the SSID profile with Source NAT action as described in Configuring Source-Based Routing on page 180. The source NAT pool is configured and source based routing entry is created.

Configuring a Destination NAT Access Rule

Instant supports configuration of the destination NAT rule, which can be used to redirect traffic to the specified IP address and destination port. Destination-NAT configuration is supported only in the bridge mode without VPN.

You can configure a destination-NAT access rule by using the Instant UI or CLI.

In the Instant UI

To configure a destination NAT access rule:

1. Navigate to the WLAN wizard or Wired settings window:
   - To configure access rules for a WLAN SSID, in the **Network** tab, click **New** to create a new network profile or **edit** to modify an existing profile.
   - To configure access rules for a wired profile, **More** > **Wired**. In the **Wired** window, click **New** under **Wired Networks** to create a new network or click **Edit** to select an existing profile.
2. Click the **Access** tab.
3. To configure access rules for the network, slide to **Network-based**. To configure access rules for user roles, slide to **Role-based** .
4. To create a new rule for the network, click **New**. To create an access rule for a user role, select the user role and then click **New**. The **New Rule** window is displayed.
5. In the **New Rule** window:
6. Select **Access control** from the **Rule type** drop-down list.
7. Select **destination-NAT** from the **Action** drop-down list, to allow changes to the source IP address.
8. Specify the IP address and port details.
9. Select a service from the list of available services.
10. Select the required option from the **Destination** drop-down list.
11. If required, enable other parameters such as **Log**, **Blacklist**, **Classify media**, **Disable scanning**, **DSCP tag**, and **802.1p priority**.
12. Click **OK** and then click **Finish**.

In the CLI

To configure destination NAT access rule:

```
(Instant AP)(config)# wlan access-rule <access_rule>
(Instant AP)(Access Rule "<access_rule>")# rule <dest> <mask> <match> <protocol> <sport>
<eport> dst-nat ip <IP-address> [<port>]
(Instant AP)(Access Rule "<access_rule>")# end
(Instant AP)# commit apply
```

Configuring ALG Protocols

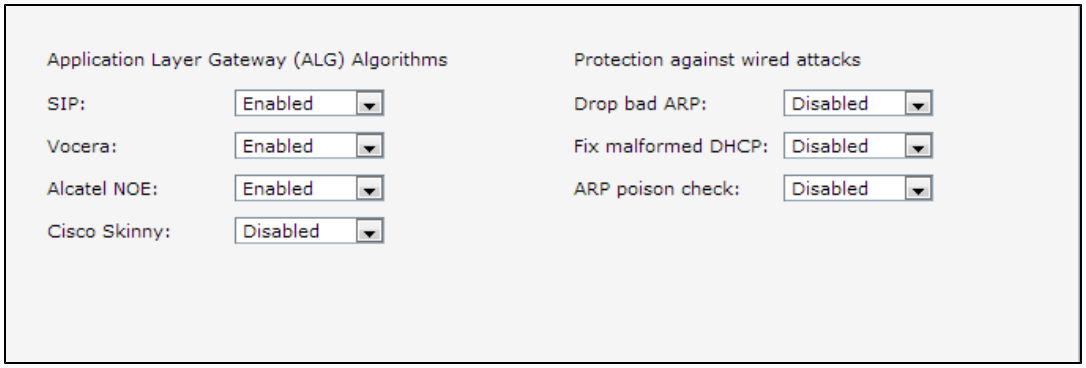
You can enable or disable protocols for Application Layer Gateway (ALG) using the Instant UI or CLI.

In the Instant UI

To configure protocols for ALG:

1. Click the **Security** link at the top right corner of Instant main window.
2. Click the **Firewall Settings** tab. The **Firewall Settings** tab contents are displayed. The following figure shows the contents of the **Firewall Settings** tab:

Figure 52 *Firewall Settings—ALG Protocols*



3. Select **Enabled** from the corresponding drop-down lists to enable SIP, VOCERA, Alcatel NOE, and Cisco skinny protocols.
4. Click **OK**.

NOTE

When the protocols for ALG are **Disabled** the changes do not take effect affect until the existing user sessions are expired. Reboot the W-IAP and the client, or wait for few minutes for changes to affect.

In the CLI

To configure protocols for ALG:

```
(Instant AP)(config)# alg
(Instant AP)(ALG)# sccp-disable
(Instant AP)(ALG)# no sip-disable
(Instant AP)(ALG)# no ua-disable
(Instant AP)(ALG)# no vocera-disable
(Instant AP)(ALG)# end
(Instant AP)# commit apply
```

To view the ALG configuration:

```
(Instant AP)# show alg

Current ALG
-----------
ALG Status
--- ------
sccp Disabled
sip Enabled
ua Enabled
vocera Enabled
```

Configuring Firewall Settings for Protection from ARP Attacks

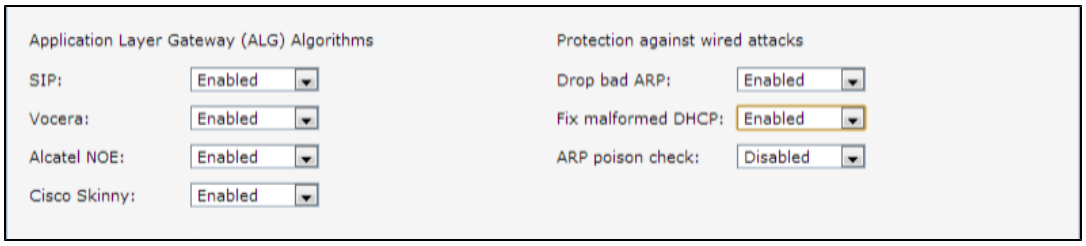
You can configure firewall settings to protect the network against attacks using the Instant UI or CLI.

In the Instant UI

To configure firewall settings:

1. Click the **Security** link at the top right corner of Instant main window.
2. Click the **Firewall Settings** tab. The **Firewall Settings** tab contents are displayed.
3. To configure protection against security attacks, select the following checkboxes:
   - Select **Drop bad ARP** to enable the W-IAP to drop the fake ARP packets.
   - Select **Fix malformed DHCP** to the W-IAP to fix the malformed DHCP packets.
   - Select **ARP poison check** to enable the W-IAP to trigger an alert notifying the user about the ARP poisoning that may have been caused by the rogue APs.

Figure 53 *Firewall Settings —Protection Against Wired Attacks*



4. Click **OK.**

In the CLI

To configure firewall settings to prevent attacks

```
(Instant AP)(config)# attack
(Instant AP)(ATTACK)# drop-bad-arp-enable
(Instant AP)(ATTACK)# fix-dhcp-enable
(Instant AP)(ATTACK)# poison-check-enable
(Instant AP)(ATTACK)# end
(Instant AP)# commit apply
```

To view the configuration status:

```
(Instant AP)# show attack config

Current Attack
--------------
Attack Status
------ ------
drop-bad-arp Enabled
fix-dhcp Enabled
poison-check Enabled
```

To view the attack statistics

```
(Instant AP)# show attack stats

attack counters
-------------------------------------
Counter Value
------- -------
arp packet counter 0
drop bad arp packet counter 0
dhcp response packet counter 0
fixed bad dhcp packet counter 0
send arp attack alert counter 0
send dhcp attack alert counter 0
arp poison check counter 0
garp send check counter 0
```

Managing Inbound Traffic

Instant now supports an enhanced inbound firewall by allowing the configuration of firewall rules and management subnets, and restricting corporate access through an uplink switch.

To allow flexibility in firewall configuration, Instant supports the following features:

- Inbound firewall rules
- Configurable management subnets
- Restricted corporate access

Configuring Inbound Firewall Rules

You can now configure firewall rules for the inbound traffic coming through the uplink ports of a W-IAP. The rules defined for the inbound traffic are applied if the destination is not a user connected to the W-IAP. If the destination already has a user role assigned, the user role overrides the actions or options specified in inbound firewall configuration. However, if a deny rule is defined for the inbound traffic, it is applied irrespective of the destination and user role. Unlike the ACL rules in a WLAN SSID or wired profile, the inbound firewall rules can be configured based on the source subnet.

For all subnets, a deny rule is created by default as the last rule. If at least one rule is configured, the deny all rule is applied to the upstream traffic by default.

Management access to the AP is allowed irrespective of the inbound firewall rule. For more information on configuring restricted management access, see Configuring Management Subnets on page 185.

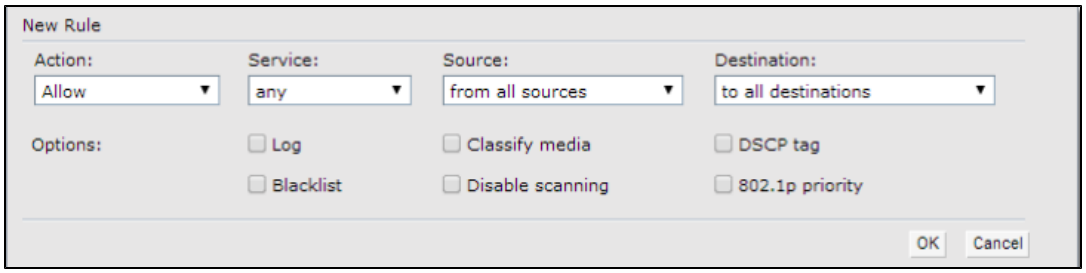
The inbound firewall is not applied to traffic coming through GRE tunnel.

You can configure inbound firewall rules through the Instant UI or CLI.

In the Instant UI

1. Navigate to **Security** > **Inbound Firewall** tab. The **Inbound Firewall** tab contents are displayed.
2. Under **Inbound Firewall Rules**, click **New**. The **New Rule** window is displayed.

Figure 54 *Inbound Firewall Rules - New Rule Window*



3. Configure the following parameters:

Table 36: *Inbound Firewall Rule Configuration Parameters*

Parameter	Description
Action	Select any of following actions: • Select **Allow** to allow access users based on the access rule. • Select **Deny** to deny access to users based on the access rule. • Select **Destination-NAT** to allow changes to destination IP address. • Select **Source-NAT** to allow changes to the source IP address. The destination-nat and source-nat actions apply only to the network services rules.
Service	Select a service from the list of available services. You can allow or deny access to any or all of the following services based on your requirement: • **any**–Access is allowed or denied to all services. • **custom**–Available options are TCP, UDP, and Other. If you select the TCP or UDP options, enter appropriate port numbers. If the **Other** option is selected, ensure enter the appropriate ID is entered.
Source	Select any of the following options: • **from all sources**– Traffic from all sources is either allowed, denied, or the IP address is translated at the source or destination as defined in the rule. • **from a host**–Traffic from a particular host is either allowed, denied, or the IP address is translated at the source or destination as defined in the rule. After selecting this option, specify the IP address of the host. • **from a network**–Traffic from a particular network is either allowed, denied, or the IP address is translated at the source or destination as defined in the rule. After selecting this option, specify the IP address and netmask of the source network.
Destination	Select a destination option for the access rules for network services, applications, and application categories. You can allow or deny access to any the following destinations based on your requirements. • **to all destinations**– Traffic for all destinations is allowed, denied, or the IP address is translated at the source or destination as defined in the rule. • **to a particular server**–Traffic to a specific server is allowed, denied, or the IP address is translated at the source or destination as defined in the rule. After selecting this option, specify the IP address of the destination server. • **except to a particular server**–Access is allowed or denied to servers other than the specified server. After selecting this option, specify the IP address of the destination server. • **to a network**–Traffic to the specified network is allowed, denied, or the IP address is translated at the source or destination as defined in the rule. After selecting this option, specify the IP address and netmask for the destination network. • **except to a network**–Access is allowed or denied to networks other than the specified network. After selecting this option, specify the IP address and netmask of the destination network. • **to domain name**–Traffic to the specified domain is allowed, denied, or the IP address is translated at the source or destination as defined in the rule. After selecting this option, specify the domain name in the **Domain Name** text box.
Log	Select this checkbox if you want a log entry to be created when this rule is triggered. Instant supports firewall based logging function. Firewall logs on the W-IAPs are generated as security logs.
Blacklist	Select the **Blacklist** checkbox to blacklist the client when this rule is triggered. The blacklisting lasts for the duration specified as **Auth failure blacklist time** on the Blacklisting tab of the **Security** window. For more information, see Blacklisting Clients on page 171.
Classify media	Select the **Classify media** checkbox to prioritize video and voice traffic. When enabled, a packet inspection is performed on all non-NAT traffic and the traffic is marked as follows: • Video: Priority 5 (Critical)

Table 36: *Inbound Firewall Rule Configuration Parameters*

Parameter	Description
	• Voice: Priority 6 (Internetwork Control)
Disable scanning	Select **Disable scanning** checkbox to disable ARM scanning when this rule is triggered. The selection of the **Disable scanning** applies only if ARM scanning is enabled, For more information, see Configuring Radio Settings for a W-IAP on page 238.
DSCP tag	Select the **DSCP tag** checkbox to specify a DSCP value to prioritize traffic when this rule is triggered. Specify a value within the range of 0 to 63. To assign a higher priority, specify a higher value.
802.1p priority	Select the **802.1p priority** checkbox to specify an 802.1p priority. Specify a value between 0 and 7. To assign a higher priority, specify a higher value.

4. Click **OK** and then click **Finish**.

In the CLI

To configure inbound firewall rules:

```
(Instant AP)(config)# inbound-firewall
(Instant AP)(inbound-firewall)# rule <subnet> <smask> <dest> <mask> <protocol> <sport> <eport>
{permit|deny|src-nat|dst-nat <IP-address> <port>} [<option1....option9>]
(Instant AP)(inbound-firewall)# end
(Instant AP)# commit apply
```

Example

```
(Instant AP)(config)# inbound-firewall
(Instant AP)(inbound-firewall)# rule 192.0.2.1 255.255.255.255 any any match 6 631 631 permit
(Instant AP)(inbound-firewall)# end
(Instant AP)# commit apply
```

Configuring Management Subnets

You can configure subnets to ensure that the W-IAP management is carried out only from these subnets. When the management subnets are configured, Telnet, SSH, and UI access is restricted to these subnets only.

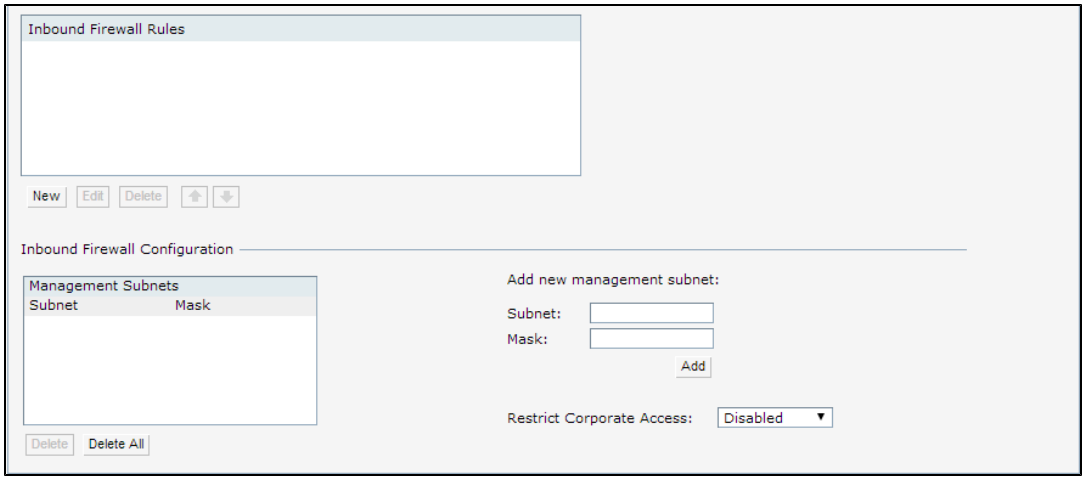
You can configure management subnets by using the Instant UI or CLI.

In the Instant UI

To configure management subnets:

1. Navigate to **Security** > **Inbound Firewall**. The **Inbound Firewall** tab contents are displayed.

Figure 55 *Firewall Settings—Management Subnets*



2. To add a new management subnet:
   - Enter the subnet address in **Subnet**.
   - Enter the subnet mask in **Mask.**
   - Click **Add**.
3. To add multiple subnets, repeat step 2.
4. Click **OK**.

In the CLI

To configure a management subnet:

```
(Instant AP)(config) # restricted-mgmt-access <subnet-IP-address> <subnet-mask>
(Instant AP)(config) # end
(Instant AP)# commit apply
```

Configuring Restricted Access to Corporate Network

You can configure restricted corporate access to block unauthorized users from accessing the corporate network. When restricted corporate access is enabled, corporate access is blocked from the uplink port of master W-IAP, including clients connected to a slave W-IAP. You can configure restricted corporate access by using the Instant UI or CLI.

In the Instant UI

To configure restricted corporate access:

1. Navigate to **Security** > **Inbound Firewall**. The **Inbound Firewall** (see Figure 55) tab contents are displayed.
2. Select **Enabled** from the **Restrict Corporate Access**.
3. Click **OK**.

In the CLI

To configure restricted management access:

```
(Instant AP)(config) # restrict-corp-access
(Instant AP)(config) # end
(Instant AP)# commit apply
```

Content Filtering

The content filtering feature allows you to route DNS request to the OpenDNS platform and create content filtering policies.

With content filter, you can:

- Allow all DNS requests to the non-corporate domains on a wireless or wired network to be sent to the open DNS server. When the OpenDNS credentials are configured, the W-IAP uses these credentials to access OpenDNS to provide enterprise-level content filtering. For more information, see Configuring OpenDNS Credentials on page 266
- Block certain categories of websites based on your organization policy. For example, if you block the **web-based-email** category, clients who are assigned this policy will not be able to visit email-based websites such as mail.yahoo.com.
- Prevent known malware hosts from accessing your wireless network.
- Improve employee productivity by limiting access to certain websites.
- Reduce bandwidth consumption significantly.

Regardless of whether content filtering is disabled or enabled, the DNS requests to instant.dell-pcw.com are always resolved internally on Instant.

The content filtering configuration applies to all W-IAPs in the network and the service is enabled or disabled globally across the wireless or wired network profiles.

Enabling Content Filtering

This section describes the following procedures:

- Enabling Content Filtering for a Wireless Profile on page 187
- Enabling Content Filtering for a Wired Profile

Enabling Content Filtering for a Wireless Profile

To enable content filtering for a wireless SSID, perform the following steps:

In the Instant UI

1. Select a wireless profile in the **Networks** tab and then click the **edit** link. The window for editing the WLAN SSID profile is displayed.
2. Click **Show advanced options**.
3. Select **Enabled** from the **Content Filtering** drop-down list, and click **Next** to continue.

You can also enable content filtering while adding a new wireless profile. For more information, see Configuring WLAN Settings for an SSID Profile on page 93.

In the CLI

To enable content filtering on a WLAN SSID:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# content-filtering
(Instant AP)(SSID Profile <name>)# end
(Instant AP)# commit apply
```

Enabling Content Filtering for a Wired Profile

To enable content filtering for a wired profile, perform the following steps:

In the Instant UI

1. Click the **Wired** link under **More** at the top right corner of the main window. The **Wired** window is displayed.
2. In the **Wired** window, select the wired profile to modify.

3. Click **Edit**. The **Edit Wired Network** window is displayed.
4. In the **Wired Settings** tab, select **Enabled** from the **Content Filtering** drop-down list and click **Next** to continue.

In the CLI

To enable content filtering for a wired profile in the CLI:

```
(Instant AP)(config)# wired-port-profile test
(Instant AP)(wired ap profile <name>)# content-filtering
(Instant AP)(wired ap profile <name>)# end
(Instant AP)# commit apply
```

Configuring Enterprise Domains

The enterprise domain names list displays the DNS domain names that are valid on the enterprise network. This list is used to determine how client DNS requests must be routed. When **Content Filtering** is enabled, the DNS request of the clients is verified and the domain names that do not match the names in the list are sent to the open DNS server.

You can configure an enterprise domain through the Instant UI or CLI.

In the Instant UI

To manually add a domain:

1. Navigate to **System** > **General**, click **Show advanced options** > **Enterprise Domains**. The **Enterprise Domain** tab contents are displayed.
2. Click **New** and enter a **New Domain Name**. Using "*" as an enterprise domain causes all DNS traffic to go through the tunnel to the original DNS server of clients. If you are configuring routing profile with split-tunnel disabled, you need add "*" to the enterprise domain list.
3. Click **OK** to apply the changes.

To delete a domain, select the domain and click **Delete** to remove the domain name from the list.

In the CLI

To configure an enterprise domain:

```
(Instant AP)(config)# internal-domains
(Instant AP)(domain)# domain-name <name>
(Instant AP)(domain)# end
(Instant AP)# commit apply
```

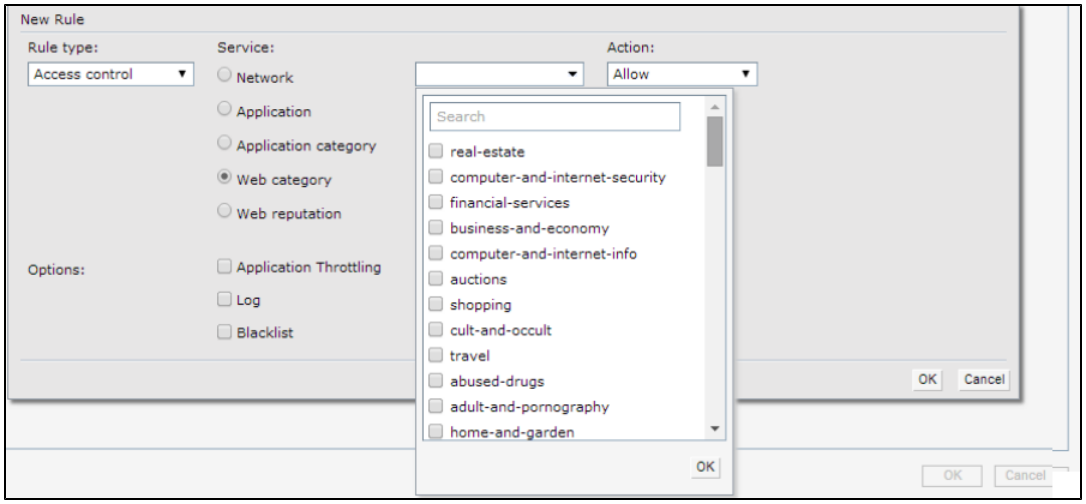
Configuring URL Filtering Policies

You can configure URL filtering policies to block certain categories of websites based on your organization specifications by defining ACL rules either through the Instant UI or CLI.

In the Instant UI

1. Navigate to **Security >Roles**.
2. Select any WLAN SSID or wired profile role, and click **New** in the Access Rules section. The **New Rule window** appears.
3. Select the rule type as **Access Control**.
4. To set an access policy based on the web category:
   a. Under **Services**, select **Web category** and expand the **Web categories** drop-down.

Figure 56



b. Select the categories to which you want to deny or allow access. You can also search for a web category and select the required option.

c. From the **Action** drop-down, select **Allow** or **Deny** as required.

d. Click **OK**.

5. To filter access based on the security ratings of the website:

   a. Select **Web reputation** under **Services**.

   b. Move the slider to the required security rating level.

   c. From the **Action** drop-down, select **Allow** or **Deny** as required.

6. To set a bandwidth limit based on web category or web reputation score, select **Application Throttling** checkbox and specify the downstream and upstream rates in Kbps. For example, you can set a higher bandwidth for trusted sites and a low bandwidth rate for high risk sites.

7. Click **OK** to save the rules.

8. Click **OK** in **Roles** tab to save the changes to the role for which you defined ACL rules.

In the CLI

To control access based on web categories and security ratings:

```
(Instant AP)(config)# wlan access-rule <access_rule>
(Instant AP) (Access Rule "<access-rule>")# rule <dest> <mask> <match> webcategory <webgrp>
{permit| deny}[<option1....option9>]
(Instant AP) (Access Rule "<access-rule>")# rule <dest> <mask> <match> webreputation <webrep>
{permit|deny}[<option1....option9>]
(Instant AP) (Access Rule "<access-rule>")# end
(Instant AP)# commit apply
```

Example

```
(Instant AP)(config)# wlan access-rule URLFilter
(Instant AP) (Access Rule "URLFilter")# rule any any match webcategory gambling deny
(Instant AP) (Access Rule "URLFilter")# rule any any match webcategory training-and-tools
permit
(Instant AP) (Access Rule "URLFilter")# rule any any match webreputation trustworthy-sites
permit
(Instant AP) (Access Rule "URLFilter")# rule any any match webreputation suspicious-sites deny
(Instant AP) (Access Rule "URLFilter")# end
(Instant AP)# commit apply
```

Configuring User Roles

Every client in the Instant network is associated with a user role, which determines the client's network privileges, the frequency of reauthentication, and the applicable bandwidth contracts.

Instant allows you to configuration of up to 32 user roles. If the number of roles exceed 32, an error message is displayed.

The user role configuration on a W-IAP involves the following procedures:

- Creating a User Role on page 190
- Assigning Bandwidth Contracts to User Roles on page 190
- Configuring Machine and User Authentication Roles on page 191

Creating a User Role

You can create a user role by using the Instant UI or CLI.

In the Instant UI

To create a user role:

1. Click the **Security** at the top right corner of Instant main window. The **Security** window is displayed.
2. Click **Roles** tab. The Roles tab contents are displayed.
3. Under Roles, click **New**.
4. Enter a name for the new role and click **OK**.

You can also create a user role when configuring wireless or wired network profiles. For more information, see Configuring Access Rules for a WLAN SSID Profile on page 104 and Configuring Access Rules for a Wired Profile on page 116

In the CLI

To configure user roles and access rules:

```
(Instant AP)(config)# wlan access-rule <access-rule-name>
(Instant AP)(Access Rule <Name>)# rule <dest> <mask> <match> <protocol> <start-port> <end-port> {permit |deny | src-nat | dst-nat {<IP-address> <port> | <port>}}[<option1…option9>]
```

Assigning Bandwidth Contracts to User Roles

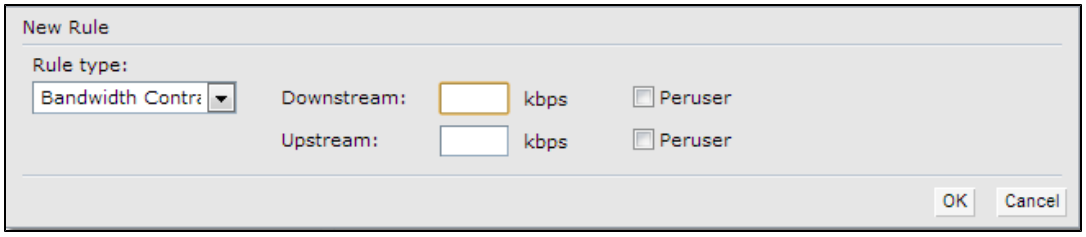
The administrators can manage bandwidth utilization by assigning maximum bandwidth rates, or bandwidth contracts to user roles. The administrator can assign a bandwidth contract configured in Kbps to upstream (client to the W-IAP) or downstream (W-IAP to clients) traffic for a user role. The bandwidth contract will not be applicable to the user traffic on the bridged out (same subnet) destinations. For example, if clients are connected to an SSID, you can restrict the upstream bandwidth rate allowed for each user to 512 Kbps.

By default, all users that belong to the same role share a configured bandwidth rate for upstream or downstream traffic. The assigned bandwidth will be served and shared among all the users. You can also assign bandwidth per user to provide every user a specific bandwidth within a range of 1 to 65535 Kbps. If there is no bandwidth contract specified for a traffic direction, unlimited bandwidth is allowed.

In the earlier releases, bandwidth contract could be assigned per SSID. In the current release, the bandwidth contract can also be assigned for each SSID user. If the bandwidth contract is assigned for an SSID in the Instant 6.2.1.0-3.4.0.0 image, and when the W-IAP is upgraded to 6.4.0.2-4.1 release version, the bandwidth configuration per SSID will be treated as a per-user downstream bandwidth contract for that SSID.

In the Instant UI

1. Click the **Security** at the top right corner of Instant main window. The **Security** window is displayed.
2. Click the **Roles** tab. The **Roles** tab contents are displayed.
3. Create a new role or select an existing role.
4. Under Access Rules, click **New**. The **New Rule** window is displayed.
5. Select **Bandwidth Contract** from the **Rule Type** drop-down list.



6. Specify the downstream and upstream rates in Kbps. If the assignment is specific for each user, select the **Peruser** checkbox.
7. Click **OK**.
8. Associate the user role to a WLAN SSID or wired profile.

You can also create a user role and assign bandwidth contracts while configuring an SSID or wired profile.

In the CLI:

To assign a bandwidth contract in the CLI:

```
(Instant AP)(config)# wlan access-rule <name>
(Instant AP) (Access Rule <name>)# bandwidth-limit {downstream <kbps>| upstream <kbps>|peruser
{downstream <kbps>| upstream <kbps>}}
(Instant AP) (Access Rule <name>)# end
(Instant AP) # commit apply
```

To associate the access rule to a wired profile:

```
(Instant AP)(config)# wired-port-profile <name>
(Instant AP)(wired ap profile <name>)# access-rule-name <access-rule-name>
(Instant AP)(wired ap profile <name>)# end
(Instant AP) # commit apply
```

Configuring Machine and User Authentication Roles

You can assign different rights to clients based on whether their hardware device supports machine authentication. Machine Authentication is only supported on Windows devices, so this can be used to distinguish between Windows devices and other devices such as iPads.

You can create any of the following types of rules:

- Machine Auth only role - This indicates a Windows machine with no user logged in. The device supports machine authentication and has a valid RADIUS account, but a user has not yet logged in and authenticated.
- User Auth only role - This indicates a known user or a non-Windows device. The device does not support machine auth or does not have a RADIUS account, but the user is logged in and authenticated.

When a device does both machine and user authentication, the user obtains the default role or the derived role based on the RADIUS attribute.

You can configure machine authentication with role-based access control using the Instant UI or CLI.

In the Instant UI

To configure machine authentication with role-based access control, perform the following steps:

1. In the **Access** tab of the WLAN (**New WLAN** or **Edit <WLAN-profile>**) or Wired Network configuration (**New Wired Network** or **Edit Wired Network**) window, under **Roles**, create **Machine auth only** and **User auth only** roles.
2. Configure access rules for these roles by selecting the role, and applying the rule. For more information on configuring access rules, see Configuring Access Rules for Network Services on page 177.
3. Select **Enforce Machine Authentication** and select the **Machine auth only** and **User auth only** roles.
4. Click **Finish** to apply these changes.

In the CLI

To configure machine and user authentication roles for a WLAN SSID:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name># set-role-machine-auth <machine-authentication-only> <user-authentication-only>
(Instant AP)(SSID Profile <name># end
(Instant AP)# commit apply
```

To configure machine and user authentication roles for wired profile:

```
(Instant AP)(config)# wired-port-profile <name>
(Instant AP)(wired ap profile <name>)# set-role-machine-auth <machine-authentication-only> <user-authentication-only>
(Instant AP)(wired ap profile <name>)# end
(Instant AP)# commit apply
```

Configuring Derivation Rules

Instant allows you to configure role and VLAN derivation-rules. You can configure these rules to assign a user role or VLAN to the clients connecting to an SSID or a wired profile.

Understanding Role Assignment Rule

When an SSID or wired profile is created, a default role for the clients connecting this SSID or wired profile is assigned. You can assign a user role to the clients connecting to an SSID by any of the following methods. The role assigned by some methods may take precedence over the roles assigned by the other methods.

RADIUS VSA Attributes

The user role can be derived from Dell Vendor-Specific Attributes (VSA) for RADIUS server authentication. The role derived from a Dell VSA takes precedence over roles defined by other methods.

MAC-Address Attribute

The first three octets in a MAC address are known as Organizationally Unique Identifier (OUI), and are purchased from the Institute of Electrical and Electronics Engineers, Incorporated (IEEE) Registration Authority. This identifier uniquely identifies a vendor, manufacturer, or other organization (referred to by the IEEE as the “assignee”) globally and effectively reserves a block of each possible type of derivative identifier (such as MAC addresses) for the exclusive use of the assignee.

W-IAPs use the OUI part of a MAC address to identify the device manufacturer and can be configures to assign a desired role for users who have completed 802.1X authentication and MAC authentication. The user role can be derived from the user attributes after a client associates with an AP. You can configure rules that assign a user role to clients that match a MAC address based criteria. For example, you can assign a voice role to any client with a MAC address starting a0:a1:a2.

Roles Based on Client Authentication

The user role can be the default user role configured for an authentication method, such as 802.1x authentication. For each authentication method, you can configure a default role for clients who are successfully authenticated using that method.

DHCP Option and DHCP Fingerprinting

The DHCP fingerprinting allows you to identify the operating system of a device by looking at the options in the DHCP frame. Based on the operating system type, a role can be assigned to the device.

For example, to create a role assignment rule with the DHCP option, select **equals** from the **Operator** drop-down list and enter 370103060F77FC in the **String** text box. Since 370103060F77FC is the fingerprint for Apple iOS devices such as iPad and iPhone, W-IAP assigns Apple iOS devices to the role that you choose.

Table 37: *Validated DHCP Fingerprint*

Device	DHCP Option	DHCP Fingerprint
Apple iOS	Option 55	370103060F77FC
Android	Option 60	3C64686370636420342E302E3135
Blackberry	Option 60	3C426C61636B4265727279
Windows 7/Vista Desktop	Option 55	37010f03062c2e2f1f2179f92b
Windows XP(SP3, Home, Professional)	Option 55	37010f03062c2e2f1f21f92b
Windows Mobile	Option 60	3c4d6963726f736f66742057696e646f777320434500
Windows 7 Phone	Option 55	370103060f2c2e2f
Apple Mac OSX	Option 55	370103060f775ffc2c2e2f

Creating a Role Derivation Rule

You can configure rules for determining the role that is assigned for each authenticated client.

When creating more than one role assignment rule, the first matching rule in the rule list is applied.

You can create a role assignment rules by using the Instant UI or CLI.

In the Instant UI

1. Navigate to the WLAN wizard or Wired settings window:
   - To configure access rules for a WLAN SSID, in the **Network** tab, click **New** to create a new network profile or **edit** to modify an existing profile.
   - To configure access rules for a wired profile, **More** > **Wired**. In the **Wired** window, click **New** under **Wired Networks** to create a new network or click **Edit** to select an existing profile.
2. Click the **Access** tab.
3. Under **Role Assignment Rules**, click **New**. The **New Role Assignment** window allows you to define a match method by which the string in *Operand* is matched with the attribute value returned by the authentication server.

4. Select the attribute from the **Attribute** drop-down list that the rule it matches against. The list of supported attributes includes RADIUS attributes, dhcp-option, dot1x-authentication-type, mac-address, and mac-address-and-dhcp-options. For information on a list of RADIUS attributes, see RADIUS Server Authentication with VSA on page 150.
5. Select the operator from the **Operator** drop-down list. The following types of operators are supported:
   - **contains**– The rule is applied only if the attribute value contains the string specified in *Operand*.
   - **Is the role**– The rule is applied if the attribute value is the role.
   - **equals**– The rule is applied only if the attribute value is equal to the string specified in *Operand*.
   - **not-equals**– The rule is applied only if the attribute value is not equal to the string specified in *Operand*.
   - **starts-with**– The rule is applied only if the attribute value starts with the string specified in *Operand*.
   - **ends-with**– The rule is applied only if the attribute value ends with string specified in *Operand*.
   - **matches-regular-expression**– The rule is applied only if the attribute value matches the regular expression pattern specified in *Operand*. This operator is available only if the **mac-address-and-dhcp-options** attribute is selected in the **Attribute** drop-down. The **mac-address-and-dhcp-options** attribute and **matches-regular-expression** are applicable only for the WLAN clients.
6. Enter the string to match in the **String** text box.
7. Select the appropriate role from the **Role** drop-down list.
8. Click **OK**.

When Enforce Machine Authentication is enabled, both the device and the user must be authenticated for the role assignment rule to apply.

In the CLI

To configure role assignment rules for a WLAN SSID:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# set-role <attribute>{{equals|not-equals|starts-with|ends-with|contains|matches-regular-expression} <operator><role>|value-of}
(Instant AP)(SSID Profile <name># end
(Instant AP)# commit apply
```

To configure role assignment rules for a wired profile:

```
(Instant AP)(config)# wired-port-profile <name>
(Instant AP)(wired ap profile <name>)# set-role <attribute>{{equals| not-equal| starts-with| ends-with|contains}<operator> <role>| value-of}
(Instant AP)(wired ap profile <name>)# end
(Instant AP)# commit apply
```

Example

```
(Instant AP)(config)# wlan ssid-profile Profile1
(Instant AP)(SSID Profile "Profile1")# set-role mac-address-and-dhcp-options matches-regular-expression \bring\b Profile1
(Instant AP)(SSID Profile"Profile1")# end
(Instant AP)# commit apply
```

Understanding VLAN Assignment

You can assign VLANs to a client based on the following configuration conditions:

- The default VLAN configured for the WLAN can be assigned to a client.
- If VLANs are configured for a WLAN SSID or an Ethernet port profile, the VLAN for the client can be derived before the authentication, from the rules configured for these profiles.
- If a rule derives a specific VLAN, it is prioritized over the user roles that may have a VLAN configured.

- The user VLANs can be derived from the default roles configured for 802.1X authentication or MAC authentication.
- After client authentication, the VLAN can be derived from Vendor Specific Attributes (VSA) for RADIUS server authentication.
- The DHCP-based VLANs can be derived for Captive Portal authentication.

NOTE

Instant supports role derivation based on the DHCP option for Captive Portal authentication. When the Captive Portal authentication is successful, the role derivation based on the DHCP option assigns a new user role to the guest users, instead of the pre-authenticated role.

Vendor Specific Attributes

When an external RADIUS server is used, the user VLAN can be derived from the **Dell-User-Vlan** VSA. The VSA is then carried in an *Access-Accept* packet from the RADIUS server. The W-IAP can analyze the return message and derive the value of the VLAN which it assigns to the user.

Figure 57 *RADIUS Access-Accept packets with VSA*

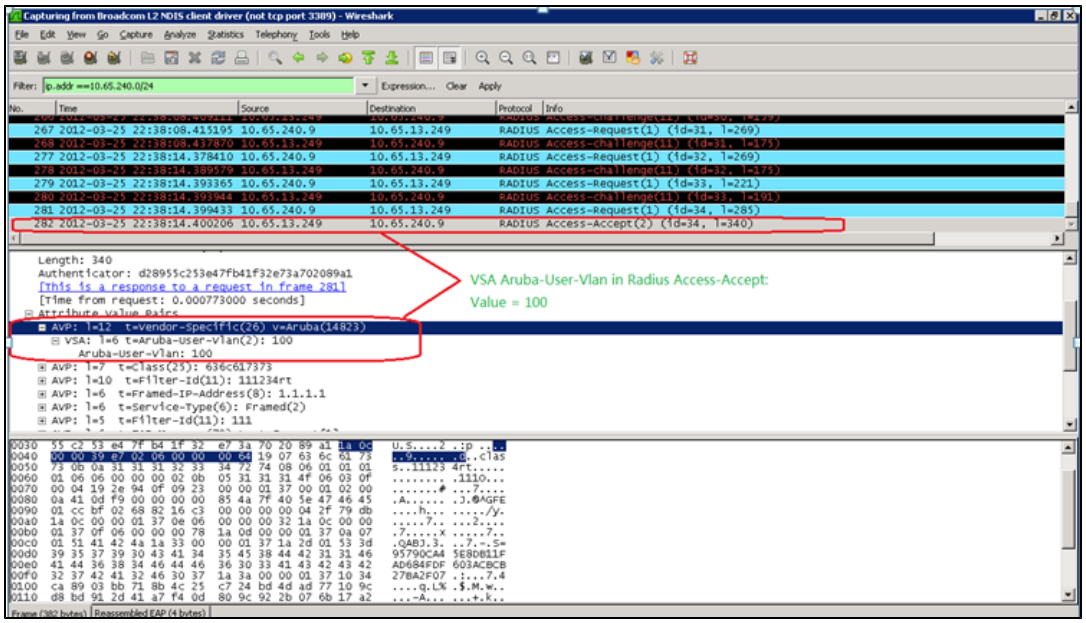
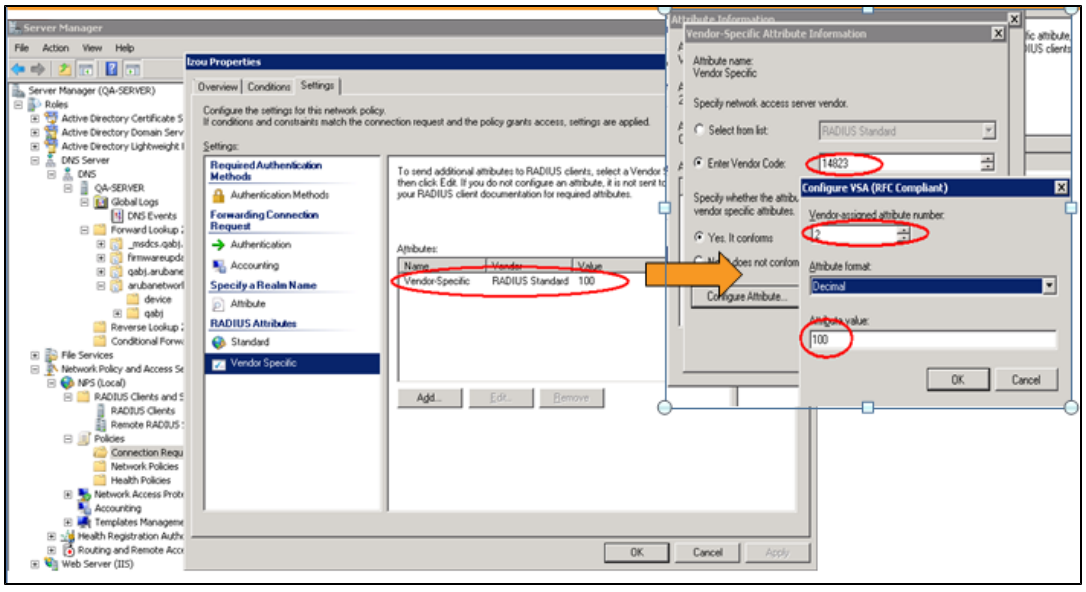


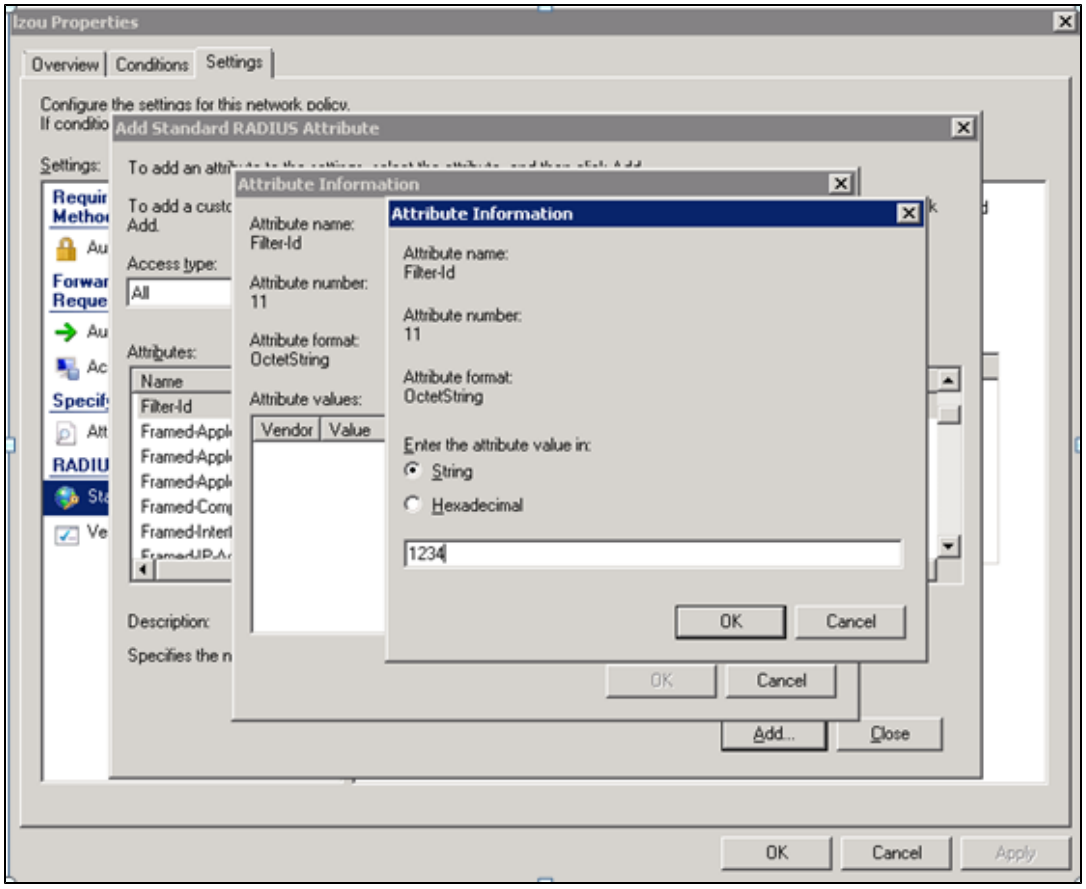
Figure 58 *Configure VSA on a RADIUS Server*



VLAN Assignment Based on Derivation Rules

When an external RADIUS server is used for authentication, the RADIUS server may return a reply message for authentication. If the RADIUS server supports return attributes, and sets an attribute value to the reply message, the W-IAP can analyze the return message and match attributes with a user pre-defined VLAN derivation rule. If the rule is matched, the VLAN value defined by the rule is assigned to the user. For a complete list of RADIUS server attributes, see RADIUS Server Authentication with VSA on page 150.

Figure 59 *Configuring RADIUS Attributes on the RADIUS Server*



User Role

If the VSA and VLAN derivation rules are not matching, then the user VLAN can be derived by a user role.

VLANs Created for an SSID

If the VSA and VLAN derivation rules are not matching, and the User Role does not contain a VLAN, the user VLAN can be derived by VLANs configured for an SSID or Ethernet port profile.

Configuring VLAN Derivation Rules

The users are assigned to a VLAN based on the attributes returned by the RADIUS server after the users authenticate.

You can configure VLAN derivation rules for an SSID profile by using the Instant UI or CLI.

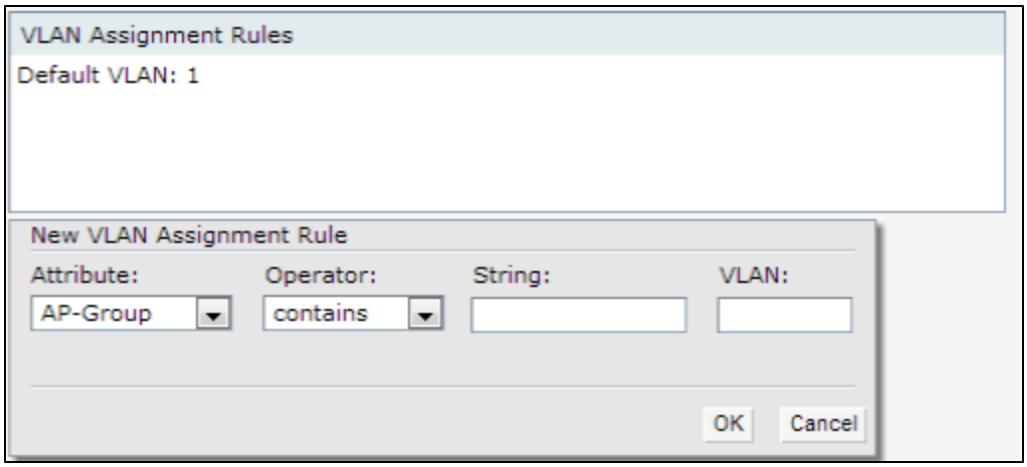
In the Instant UI

1. Perform the following steps:

- To configure VLAN derivation rule for a WLAN SSID profile, Click **Network** > **New** > **New WLAN** > **VLAN** or **Network** > **edit** > **Edit <WLAN-profile>** > **VLAN**. Select the **Dynamic** option under the **Client VLAN assignment**.
- To configure VLAN derivation rule for a wired network profile, click **Wired** > **New** > **New Wired Network** > **VLAN** or **Wired** > **Edit** > **Edit Wired Network** > **VLAN**.

2. Click **New** to create a VLAN assignment rule. The **New VLAN Assignment Rule** window is displayed. In this window, you can define a match method by which the string in *Operand* is matched with the attribute values returned by the authentication server.

Figure 60 *VLAN Assignment Rule Window*



3. Select the attribute from the **Attribute** drop-down list. The list of supported attributes includes RADIUS attributes, dhcp-option, dot1x-authentication-type, mac-address, and mac-address-and-dhcp-options. For information on a list of RADIUS attributes, see RADIUS Server Authentication with VSA on page 150.
4. Select the operator from the **Operator** drop-down list. The following types of operators are supported:
   - **contains**– The rule is applied only if the attribute value contains the string specified in *Operand*.
   - **equals**– The rule is applied only if the attribute value is equal to the string specified in *Operand*.
   - **not-equals** – The rule is applied only if the attribute value is not equal to the string specified in *Operand*.
   - **starts-with** – The rule is applied only if the attribute value starts with the string specified in *Operand*.
   - **ends-with** – The rule is applied only if the attribute value ends with string specified in *Operand*.
   - **matches-regular-expression** – The rule is applied only if the attribute value matches the regular expression pattern specified in *Operand*. This operator is available only if the **mac-address-and-dhcp-options** attribute is selected in the **Attribute** drop-down. The **mac-address-and-dhcp-options** attribute and **matches-regular-expression** are applicable only for the WLAN clients.
5. Enter the string to match in the **String** field.
6. Select the appropriate VLAN ID from the **VLAN** drop-down list.
7. Click **OK**.
8. Ensure that all other required parameters are configured.
9. Click **Finish** to apply the changes.

In the CLI

To create a VLAN assignment rule for WLAN SSID:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# set-vlan <attribute>{equals|not-equals|starts-with|ends-with|contains|matches-regular-expression}<operator><VLAN-ID>|value-of}
(Instant AP)(SSID Profile <name>)# end
(Instant AP)# commit apply
```

To configure a VLAN assignment rule for a wired profile:

```
(Instant AP)(config)# wired-port-profile <nname>
(Instant AP)(wired ap profile <name>)# set-vlan <attribute>{equals|not-equals|starts-with|ends-with|contains}<operator><VLAN-ID>|value-of}
(Instant AP)(wired ap profile <name>)# end
(Instant AP)# commit apply
```

Example

```
(Instant AP)(config)# wlan ssid-profile Profile1
(Instant AP)(SSID Profile "Profile1")# set-vlan mac-address-and-dhcp-options matches-regular-expression ..link 100
(Instant AP)(SSID Profile "Profile1")# end
(Instant AP)# commit apply
```

Using Advanced Expressions in Role and VLAN Derivation Rules

For complex policies of role and VLAN derivation using device DHCP fingerprints, you can use a regular expression to match against the combined string of the MAC address and the DHCP options. The combined string is formed by concatenating the hexadecimal presentation of the MAC address and all of the DHCP options sent by a particular device. The regular expression is a powerful pattern description language that can be used to perform advanced pattern matching of the above string.

If the combined device fingerprint string matches the specified regular expression, the role or vlan can be set to the WLAN client.

The following table lists some of the most commonly used regular expressions, which can be used in user role and user VLAN derivation rules:

Operator	Description
.	Matches any character. For example, l..k matches lack, lark, link, lock, look, Lync and so on.
\	Matches the character that follows the backslash. For example, \192.\.0\.. matches IP addresses ranges that starting with 192.0, such as 192.0.1.1. The expression looks only for the single characters that match.
[ ]	Matches any one character listed between the brackets. For example, [bc]lock matches block and clock.
\b	Matches the words that begin and end with the given expression. For example, \bdown matches downlink, linkdown, shutdown.
\B	Matches the middle of a word. For example, \Bvice matches services, devices, serviceID, deviceID, and so on.
^	Matches the characters at starting position in a string. For example, ^bcd matches bcde or bcdf, but not abcd.
[^]	Matches any characters that are not listed between the brackets. For example, [^u]link matches downlink, link, but not uplink.
?	Matches any one occurrence of the pattern. For example, ?est matches best, nest, rest, test and so on.
$	Matches the end of an input string. For example, eth$ matches Eth, but not Ethernet.
*	Matches the declared element multiple times if it exists. For example, eth* matches all occurrences of eth, such as Eth, Ethernet, Eth0 and so on.

Operator	Description
+	Matches the declared element one or more times. For example, aa+ matches occurrences of aa and aaa.
( )	Matches nested characters. For example, (192)* matches any number of the character string 192.
|	Matches the character patterns on either side of the vertical bar. You can use this expression to construct a series of options.
\<	Matches the beginning of the word. For example, \<wire matches wired, wireless and so on.
\>	Matches the end of the word. For example, \>list matches blacklist, whitelist, and so on.
{n}	Where n is an integer" Matches the declared element exactly the n times. For example, {2}link matches uplink, but not downlink.
{n,}	Where n is an integer" Matches the declared element at n times. For example, {2,}ink matches downlink, but not uplink.

For information on how to use regular expressions in role and VLAN derivation rules, see the following topics:

- Configuring VLAN Derivation Rules on page 196
- Creating a Role Derivation Rule on page 193

Configuring a User Role for VLAN Derivation

This section describes the following procedures:

- Creating a User VLAN Role on page 199
- Assigning User VLAN Roles to a Network Profile on page 200

Creating a User VLAN Role

You can create a user role for VLAN derivation using the Instant UI or CLI

In the Instant UI

To configure a user role for VLAN derivation:

1. Click the **Security** at the top right corner of Instant main window.
2. Click the **Roles** tab. The Roles tab contents are displayed.
3. Under Roles, click **New**.
4. Enter a name for the new role and click **OK**.
5. Under the **Access rules**, click **New**.
6. Select the **Rule type** as **VLAN assignment**.
7. Enter the ID of the VLAN in the **VLAN ID** text box.
8. Click **OK**.

In the CLI

To create a VLAN role:

```
(Instant AP)(config)# wlan access-rule <rule-name>
(Instant AP)(Access Rule <rule-name>)# vlan 200
(Instant AP)(Access Rule <rule-name>)# end
(Instant AP)# commit apply
```

Assigning User VLAN Roles to a Network Profile

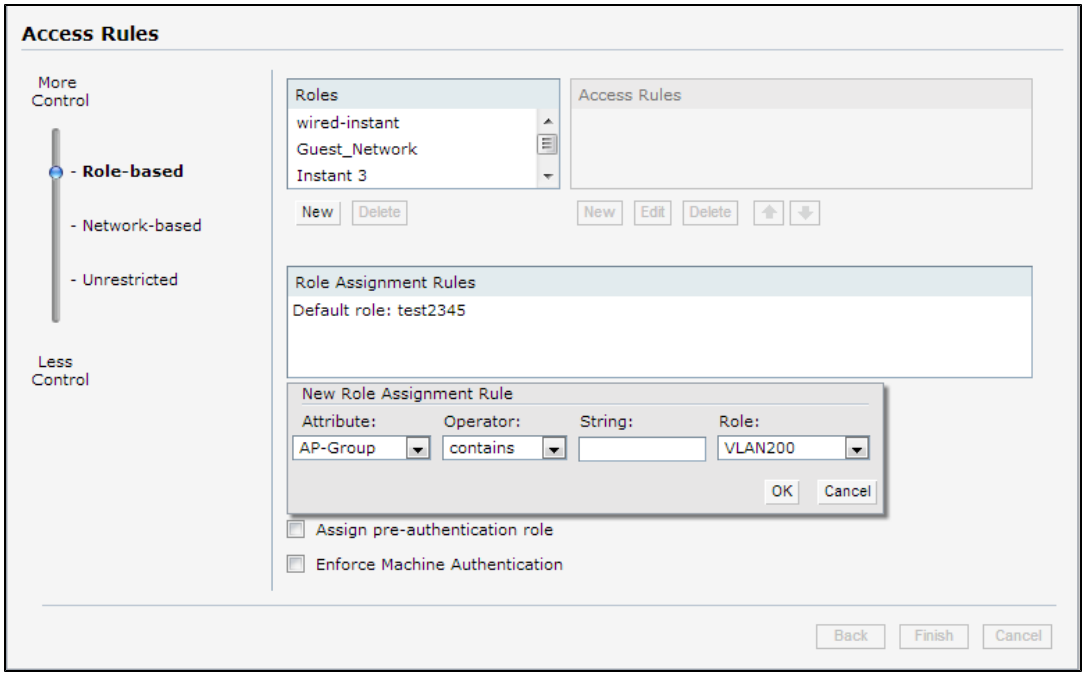
You can configure user VLAN roles for a network profile using Instant UI or CLI.

In the Instant UI

To assign a user VLAN role:

1. Click **Network** > **New** > **New WLAN** > **Access** or **Network** > **edit** > **Edit <WLAN-profile>** > **Access**.
2. Ensure that the slider is at the **Role-based** option.
3. Click **New** under the **New Role Assignment** and configure the following parameters:
   a. Select the attribute from the **Attribute** drop-down list.
   b. Select the operator to match from the **Operator** drop-down list.
   c. Enter the string to match in the **String** text box.
   d. Select the role to be assigned from the **Role** text box. The following figure shows an example for the VLAN role assignment:

Figure 61 *User VLAN Role Assignment*



4. Click **OK**.

In the CLI

To assign VLAN role to a WLAN profile:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# set-role <attribute>{{equals <operator> <role>| not-equals
<operator> <role>| starts-with <operator> <role>| ends-with <operator> <role>| contains
<operator> <role>}|value-of}
(Instant AP)(SSID Profile <name>)# end
(Instant AP)# commit apply
```

This chapter provides the following information:

- Configuring DHCP Scopes on page 201
- Configuring the Default DHCP Scope for Client IP Assignment on page 208

Configuring DHCP Scopes

The virtual controller supports different modes of DHCP address assignment. With each DHCP address assignment mode, various client traffic forwarding modes are associated. For more information on client traffic forwarding modes for IAP-VPN, see IAP-VPN Forwarding Modes on page 224.

You can configure the default DHCP scope for virtual controller assigned networks, Distributed L2, Distributed L3, Local or NAT DHCP, Local L3, and Centralized DHCP scopes through the Instant UI or CLI.

This section describes the following procedures:

- Configuring the Default DHCP Scope for Client IP Assignment on page 208
- Configuring Distributed DHCP Scopes on page 201
- Configuring a Centralized DHCP Scope on page 204
- Configuring Local and Local,L3 DHCP Scopes on page 206

Configuring Distributed DHCP Scopes

Instant allows you to configure the DHCP address assignment for the branches connected to the corporate network through VPN. You can configure the range of DHCP IP addresses used in the branches and the number of client addresses allowed per branch. You can also specify the IP addresses that must be excluded from those assigned to clients, so that they are assigned statically.

Instant supports the following distributed DHCP scopes:

- **Distributed, L2** – In this mode, the Virtual Controller acts as the DHCP server, but the default gateway is in the data center. Based on the number of clients specified for each branch, the range of IP addresses is divided. Based on the IP address range and client count configuration, the DHCP server in the Virtual Controller controls a scope that is a subset of the complete IP Address range for the subnet distributed across all the branches. This DHCP Assignment mode is used with the L2 forwarding mode.
- **Distributed, L3** – In this mode, the Virtual Controller acts as the DHCP server and the default gateway. Based on the number of clients specified for each branch, the range of IP addresses is divided. Based on the IP address range and client count configuration, the DHCP server in the Virtual Controller is configured with a unique subnet and a corresponding scope.

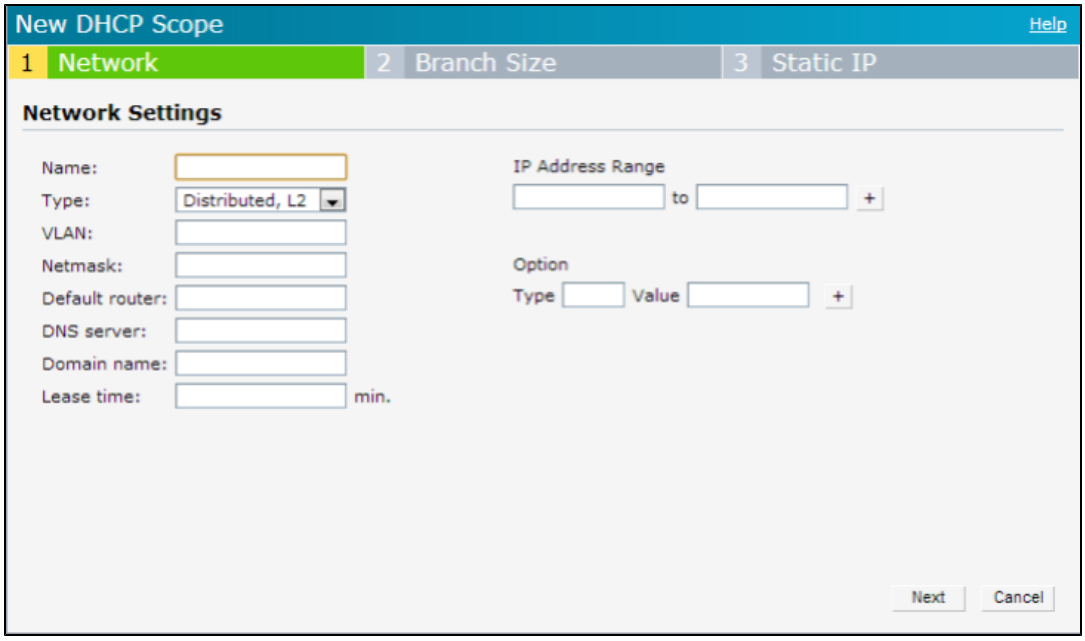
You can configure distributed DHCP scopes such as Distributed, L2 or Distributed,L3 by using the Instant UI or CLI.

In the Instant UI

To configure distributed DHCP scopes such as Distributed,L2 or Distributed,L3:

1. Click **More** > **DHCP Server**. The **DHCP Server** window is displayed.
2. To configure a distributed DHCP mode, click **New** under **Distributed DHCP Scopes**. The **New DHCP Scope** window is displayed. The following figure shows the contents of the **New DHCP Scope** window.

Figure 62 *New DHCP Scope: Distributed DHCP Mode*



3. Based on the type of distributed DHCP scope, configure the following parameters:

Table 38: *Distributed DHCP Mode: Configuration Parameters*

Name	Description
Name	Enter a name for the DHCP scope.
Type	Select any of the following options: • **Distributed, L2**– On selecting **Distributed, L2**, the Virtual Controller acts as the DHCP Server but the default gateway is in the data center. Traffic is bridged into VPN tunnel. • **Distributed, L3**– On selecting **Distributed, L3**, the Virtual Controller acts as both DHCP Server and default gateway. Traffic is routed into the VPN tunnel.
VLAN	Specify a VLAN ID. To use this subnet, ensure that the VLAN ID specified here is assigned to an SSID profile. For more information on SSID profile configuration, see Configuring VLAN Settings for a WLAN SSID Profile on page 97 and Configuring VLAN for a Wired Profile on page 114
Netmask	If **Distributed, L2** is selected for type of DHCP scope, specify the subnet mask. The subnet mask and the network determine the size of subnet.
Default router	If **Distributed, L2** is selected for type of DHCP scope, specify the IP address of the default router.
DNS Server	If required, specify the IP address of a DNS server.
Domain Name	If required, specify the domain name.

Table 38: *Distributed DHCP Mode: Configuration Parameters*

Name	Description
Lease Time	Specify a lease time for the client in minutes.
IP Address Range	Specify a range of IP addresses to use. To add another range, click the + icon. You can specify up to four different ranges of IP addresses. • For Distributed, L2 mode, ensure that all IP ranges are in the same subnet as the default router. On specifying the IP address ranges, a subnet validation is performed to ensure that the specified ranges of IP address are in the same subnet as the default router and subnet mask. The configured IP range is divided into blocks based on the configured client count. • For Distributed,L3 mode, you can configure any discontiguous IP ranges. The configured IP range is divided into multiple IP subnets that are sufficient to accommodate the configured client count. **NOTE:** You can allocate multiple branch IDs (BID) per subnet. The W-IAP generates a subnet name from the DHCP IP configuration, which the controller can use as a subnet identifier. If static subnets are configured in each branch, all of them are assigned the with BID 0, which is mapped directly to the configured static subnet.
Option	Specify the type and a value for the DHCP option. You can configure the organization-specific DHCP options supported by the DHCP server. For example, 176, 242, 161, and so on. To add multiple DHCP options, click the + icon. You can add up to eight DHCP options.

4. Click **Next**.
5. Specify the number of clients to use per branch. The client count configured for a branch determines the use of IP addresses from the IP address range defined for a DHCP scope. For example, if 20 IP addresses are available in an IP address range configured for a DHCP scope and a client count of 9 is configured, only a few IP addresses (in this example, 9) from this range will be used and allocated to a branch. The W-IAP does not allow the administrators to assign the remaining IP addresses to another branch, although a lower value is configured for the client count.
6. Click **Next**. The **Static IP** tab is displayed. Specify the number of first and last IP addresses to reserve in the subnet.
7. Click **Finish**.

In the CLI

To configure Distributed,L2 DHCP scope:

```
(Instant AP)(config)# ip dhcp <profile-name>
(Instant AP)(DHCP Profile <profile-name>)# ip dhcp server-type <Distributed,L2>
(Instant AP)(DHCP Profile <profile-name>)# server-vlan <vlan-ID>
(Instant AP)(DHCP Profile <profile-name>)# subnet-mask <subnet-mask>
(Instant AP)(DHCP Profile <profile-name>)# default-router <IP-address>
(Instant AP)(DHCP Profile <profile-name>)# client-count <number>
(Instant AP)(DHCP Profile <profile-name>)# dns-server <name>
(Instant AP)(DHCP Profile <profile-name>)# domain-name <domain-name>
(Instant AP)(DHCP Profile <profile-name>)# lease-time <minutes>
(Instant AP)(DHCP Profile <profile-name>)# ip-range <start-IP> <end-IP>
(Instant AP)(DHCP Profile <profile-name>)# reserve {first|last} <count>
(Instant AP)(DHCP Profile <profile-name>)# option <type> <value>
(Instant AP)(DHCP Profile <profile-name>)# end
(Instant AP)# commit apply
```

To configure Distributed,L3 DHCP scope:

```
(Instant AP)(config)# ip dhcp <profile-name>
(Instant AP)(DHCP Profile <profile-name>)# ip dhcp server-type <Distributed,L3>
```

```
(Instant AP)(DHCP Profile <profile-name>)# server-vlan <vlan-ID>
(Instant AP)(DHCP Profile <profile-name>)# client-count <number>
(Instant AP)(DHCP Profile <profile-name>)# dns-server <name>
(Instant AP)(DHCP Profile <profile-name>)# domain-name <domain-name>
(Instant AP)(DHCP Profile <profile-name>)# lease-time <minutes>
(Instant AP)(DHCP Profile <profile-name>)# ip-range <start-IP> <end-IP>
(Instant AP)(DHCP Profile <profile-name>)# reserve {first | last} <count>
(Instant AP)(DHCP Profile <profile-name>)# option <type> <value>
(Instant AP)(DHCP Profile <profile-name>)# end
(Instant AP)# commit apply
```

Configuring a Centralized DHCP Scope

You can configure centralized,L2 and centralized,L3 DHCP profiles. When a centralized DHCP scope is configured:

- The Virtual Controller does not assign an IP address to the client and the DHCP traffic is directly forwarded to the DHCP Server.
- For Centralized, L2 clients, the Virtual Controller bridges the DHCP traffic to the controller over the VPN/GRE tunnel. The IP address is obtained from the DHCP server behind the controller serving the VLAN/GRE of the client. This DHCP assignment mode also allows you to add the DHCP option 82 to the DHCP traffic forwarded to the controller.
- For Centralized, L3 clients, the Virtual Controller acts as a DHCP relay agent that forwards the DHCP traffic to the DHCP server located either in the corporate or local network. The centralized L3 VLAN IP is used as the source IP. The IP address is obtained from the DHCP server.

You can configure a centralized DHCP scope through the Instant UI or CLI.

In the Instant UI

To configure a centralized DHCP scope:

1. Click **More** > **DHCP Server**. The **DHCP Server** window is displayed.
2. To configure a centralized DHCP scopes, click **New** under **Centralized DHCP Scopes**. The **New DHCP Scope** window is displayed.
3. To configure centralized,L2 profile, select the profile type as **Centralized,L2** or **Centralized,L3** and configure the following parameters.

Table 39: *Centralized DHCP Mode: Configuration Parameters*

Name	Description
Name	Enter a name for the DHCP scope.
Type	Set the type as follows: • **Centralized,L2** for the centralized,L2 profile • **Centralized,L3** for the centralized,L3 profile
VLAN	Specify a VLAN ID. To use this subnet, ensure that the VLAN ID specified here is assigned to an SSID profile. For more information on SSID profile configuration, see Configuring VLAN Settings for a WLAN SSID Profile on page 97 and Configuring VLAN for a Wired Profile on page 114.
Split tunnel	Set this to **Enabled** or **Disabled** for split tunnel functionality for the centralized,L2 subnet.

Table 39: *Centralized DHCP Mode: Configuration Parameters*

Name	Description
	Enabling split tunnel allows a VPN user to access a public network and a local LAN or WAN network at the same time through the same physical network connection. For example, a user can use a remote access VPN software client connecting to a corporate network using a home wireless network. The user with split tunneling enabled is able to connect to file servers, database servers, mail servers and other servers on the corporate network through the VPN connection. When the user connects to Internet resources (Web sites, FTP sites and so on), the connection request goes directly out the gateway provided by the home network. The split-DNS functionality intercepts DNS requests from clients for non-corporate domains (as configured in Enterprise Domains list) and forwards to AP's own DNS server. When split-tunnel is disabled, all the traffic including the corporate and Internet traffic is tunneled irrespective of the routing profile specifications. If the GRE tunnel is down and when the corporate network is not reachable, the client traffic is dropped.
DHCP relay	If you are configuring a Centralized, L2 DHCP profile, you can select **Enabled** to allow the W-IAPs to intercept the broadcast packets and relay DHCP requests to centralized DHCP server. **NOTE:** The **DHCP relay** option is not available for centralized,L3 profile configuration.
Helper address	Specify the IP address of the DHCP server. **NOTE:** For Centralized, L2 DHCP profiles, the **Helper address** option is displayed only when DHCP relay is enabled.
VLAN IP	Specify the Centralized L3 DHCP subnet gateway IP.
VLAN Mask	Specify the subnet mask of the Centralized L3 DHCP subnet gateway IP.
Option82	Select **Alcatel** to enable DHCP Option 82 to allow clients to send DHCP packets with the Option 82 string. The Option 82 string is available only in the Alcatel (ALU) format. The ALU format for the Option 82 string consists of the following: • Remote Circuit ID; X AP-MAC; SSID; SSID-Type • Remote Agent; X IDUE-MAC **NOTE:** The Option 82 string is specific to Alcatel and is not configurable.

4. Click **OK**.

The following table describes the behavior of the DHCP Relay Agent and Option 82 in the W-IAP.

Table 40: *DHCP Relay and Option 82*

DHCP Relay	Option 82	Behavior
Enabled	Enabled	DHCP packet relayed with the ALU-specific Option 82 string
Enabled	Disabled	DHCP packet relayed without the ALU-specific Option 82 string
Disabled	Enabled	DHCP packet not relayed, but broadcast with the ALU-specific Option 82 string
Disabled	Disabled	DHCP packet not relayed, but broadcast without the ALU-specific Option 82 string

In the CLI

To configure a centralized,L2 DHCP profile:

```
(Instant AP)(config)# ip dhcp <profile-name>
(Instant AP)(DHCP Profile <profile-name>)# server-type <centralized>
```

```
(Instant AP)(DHCP Profile <profile-name>)# server-vlan <vlan-ID>
(Instant AP)(DHCP Profile <profile-name>)# option82 alu
(Instant AP)(DHCP Profile <profile-name>)# disable-split-tunnel
(Instant AP)(DHCP Profile <profile-name>)# end
(Instant AP)# commit apply
```

To configure a centralized,L3 DHCP profile:

```
(Instant AP)(config)# ip dhcp <profile-name>
(Instant AP)(DHCP Profile <profile-name>)# server-type <centralized>
(Instant AP)(DHCP Profile <profile-name>)# server-vlan <vlan-ID>
(Instant AP)(DHCP Profile <profile-name>)# dhcp-relay
(Instant AP)(DHCP Profile <profile-name>)# dhcp-server <DHCP-relay-server>
(Instant AP)(DHCP Profile <profile-name>)# vlan-ip <DHCP IP address> mask <VLAN mask>
(Instant AP)(DHCP Profile <profile-name>)# end
(Instant AP)# commit apply
```

Configuring Local and Local,L3 DHCP Scopes

You can configure Local and Local,L3 DHCP scopes through the Instant UI or CLI.

- **Local** – In this mode, the Virtual Controller acts as both the DHCP Server and the default gateway. The configured subnet and the corresponding DHCP scope are independent of subnets configured in other W-IAP clusters. The Virtual Controller assigns an IP address from a local subnet and forwards traffic to both **corporate** and **non-corporate** destinations. The network address is translated appropriately and the packet is forwarded through the IPSec tunnel or through the uplink. This DHCP assignment mode is used for the NAT forwarding mode.
- **Local, L3**– This DHCP assignment mode is used with the L3 forwarding mode. In this mode, the Virtual Controller acts as a DHCP server and the gateway, and assigns an IP address from the local subnet. The W-IAP routes the packets sent by clients on its uplink. The Local, L3 subnets can now access corporate network through the IPsec tunnel. The network address for all traffic generated by clients in Local, L3 subnets are translated at the source by using the tunnel inner IP to the corporate subnet. However, if corporate access to Local, L3 is not required, you can configure ACL rules to deny access.

In the Instant UI

To configure a Local or Local,L3 DHCP scope:

1. Click **More** > **DHCP Server**. The **DHCP Server** window is displayed.
2. To configure a **Local** or **Local,L3** DHCP scopes, click **New** under **Local DHCP Scopes**. The **New DHCP Scope** window is displayed.
3. Based on type of DHCP scope selected, configure the following parameters:

Table 41: *DHCP Mode: Configuration Parameters*

Name	Description
Name	Enter a name for the DHCP scope.
Type	Select any of the following options: • **Local**– On selecting **Local**, the DHCP server for local branch network is used for keeping the scope of the subnet local to the W-IAP. In the NAT mode, the traffic is forwarded through the IPSec tunnel or the uplink. • **Local, L3**–On selecting **Local, L3**, the Virtual Controller acts as a DHCP server and gateway. In this mode, the W-IAP routes the packets sent by clients and also adds a route on the controller, after the VPN tunnel is set up during the registration of the subnet.
VLAN	Specify a VLAN ID. To use this subnet, ensure that the VLAN ID specified here is assigned to an SSID profile. For more information on SSID profile configuration, see Configuring VLAN Settings for a WLAN SSID Profile on page 97 and Configuring VLAN for a Wired Profile on page 114
Network	Specify the network to use.
Netmask	If **Local** or **Local,L3** is selected, specify the subnet mask. The subnet mask and the network determine the size of subnet.
Excluded address	If **Local,L3** is selected, specify the IP address to exclude. The value entered in the field determines the exclusion range of the subnet. Based on the size of the subnet, the lesser range of IP's before or after the specified IP address will be excluded
DNS Server	If required, specify the IP address of a DNS server for the **Local** and **Local,L3** scopes.
Domain Name	If required, specify the domain name for the **Local** and **Local,L3** scopes.
Lease Time	Specify a lease time for the client in minutes.
Option	Specify the type and a value for the DHCP option. You can configure the organization-specific DHCP options supported by the DHCP server. For example, 176, 242, and 161. To add multiple DHCP options, click the + icon.

4. Click **OK**.

In the CLI

To configure Local DHCP scope:

```
(Instant AP)(config)# ip dhcp <profile-name>
(Instant AP)(DHCP Profile <profile-name>)# server-type <Local>
(Instant AP)(DHCP Profile <profile-name>)# server-vlan <vlan-ID>
(Instant AP)(DHCP Profile <profile-name>)# subnet <IP-address>
(Instant AP)(DHCP Profile <profile-name>)# subnet-mask <subnet-mask>
(Instant AP)(DHCP Profile <profile-name>)# dns-server <name>
(Instant AP)(DHCP Profile <profile-name>)# domain-name <domain-name>
(Instant AP)(DHCP Profile <profile-name>)# lease-time <minutes>
(Instant AP)(DHCP Profile <profile-name>)# option <type> <value>
(Instant AP)(DHCP Profile <profile-name>)# end
(Instant AP)# commit apply
```

To configure Local,L3 DHCP scope:

```
(Instant AP)(config)# ip dhcp <profile-name>
(Instant AP)(DHCP Profile <profile-name>)# server-type <Local,L3>
(Instant AP)(DHCP Profile <profile-name>)# server-vlan <vlan-ID>
```

```
(Instant AP)(DHCP Profile <profile-name>)# subnet <IP-address>
(Instant AP)(DHCP Profile <profile-name>)# subnet-mask <subnet-mask>
(Instant AP)(DHCP Profile <profile-name>)# exclude-address <IP-address>
(Instant AP)(DHCP Profile <profile-name>)# dns-server <name>
(Instant AP)(DHCP Profile <profile-name>)# domain-name <domain-name>
(Instant AP)(DHCP Profile <profile-name>)# lease-time <minutes>
(Instant AP)(DHCP Profile <profile-name>)# option <type> <value>
(Instant AP)(DHCP Profile <profile-name>)# end
(Instant AP)# commit apply
```

Configuring the Default DHCP Scope for Client IP Assignment

The DHCP server is a built-in server, used for networks in which clients are assigned IP address by the Virtual Controller. You can customize the DHCP pool subnet and address range to provide simultaneous access to more number of clients. The largest address pool supported is 2048. The default size of the IP address pool is 512.

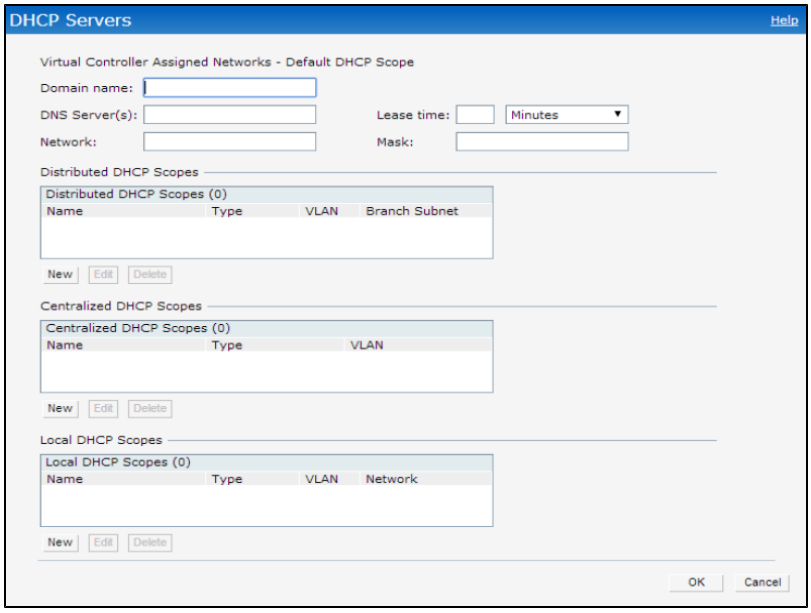
When the DHCP server is configured and if the **Client IP assignment** parameter for an SSID profile is set to **Virtual Controller Assigned**, the Virtual Controller assigns the IP addresses to the WLAN or wired clients. By default, the W-IAP automatically determines a suitable DHCP pool for **Virtual Controller Assigned** networks. In the current release, the W-IAP typically selects the 172.31.98.0/23 subnet. If the IP address of the W-IAP is within the 172.31.98.0/23 subnet, the W-IAP selects the 10.254.98.0/23 subnet. However, this mechanism does not guarantee that it would avoid all possible conflicts with the wired network. If your wired network uses either 172.31.98.0/23 or 10.254.98.0/23, and you experience problems with the **Virtual Controller Assigned** networks after upgrading to Dell Networking W-Series Instant 6.2.1.0-3.4 or later, manually configure the DHCP pool by following the steps described in this section.

You can configure a domain name, DNS server, and DHCP server for client IP assignment using the Instant UI or CLI.

In the Instant UI

1. Navigate to **More** > **DHCP Server** tab. The **DHCP Server** tab contents are displayed.

Figure 63 *DHCP Servers Window*



2. Enter the domain name of the client in the **Domain name** text box.
3. Enter the IP addresses of the DNS servers separated by a comma(,) in the **DNS server (s)** text box.

4. Enter the duration of the DHCP lease in the **Lease time** text box.
5. Select **Minutes**, **Hours**, or **Days** for the lease time from the drop-down list next to **Lease time**. The default lease time is 0.
6. Enter the network range for the client IP addresses in the **Network** field. The system generates a network range automatically that is sufficient for 254 addresses. If you want to provide simultaneous access to more number of clients, specify a larger range.
7. Specify the subnet mask details for the network range in the **Mask** text box.

The DNS cache function is only enabled when content-filtering is disabled.

8. Click **OK** to apply the changes.

In the CLI

To configure a DHCP pool:

```
(Instant AP)(config)# ip dhcp pool
(Instant AP)(DHCP)# domain-name <domain>
(Instant AP)(DHCP)# dns-server <DNS-IP-address>
(Instant AP)(DHCP)# lease-time <lease-time>
(Instant AP)(DHCP)# subnet <IP-address>
(Instant AP)(DHCP)# subnet-mask <subnet-mask>
```

To view the DHCP database:

```
(Instant AP)# show ip dhcp database

DHCP Subnet :192.0.2.0
DHCP Netmask :255.255.255.0
DHCP Lease Time(m) :20
DHCP Domain Name :example.com
DHCP DNS Server :192.0.2.1
```

This chapter describes the following VPN configuration procedures:

- Understanding VPN Features on page 210
- Configuring a Tunnel from a W-IAP to Dell Networking W-Series Mobility Controller on page 210
- Configuring Routing Profiles on page 221

Understanding VPN Features

As W-IAPs use a Virtual Controller architecture, the W-IAP network does not require a physical controller to provide the configured WLAN services. However, a physical controller is required for terminating Virtual Private Networks (VPN) tunnels from the W-IAP networks at branch locations to datacenters, where the Dell controller acts as a VPN concentrator.

When the VPN is configured, the W-IAP acting as the Virtual Controller creates a VPN tunnel to a Dell Networking W-Series mobility controller in your corporate office. The controller acts as a VPN end-point and does not supply the W-IAP with any configuration.

The VPN features are recommended for:

- Enterprises with many branches that do not have a dedicated VPN connection to the corporate office.
- Branch offices that require multiple APs.
- Individuals working from home, connecting to the VPN.

The survivability feature of W-IAPs with the VPN connectivity of W-IAPs allows you to provide corporate connectivity on non-corporate networks.

Configuring a Tunnel from a W-IAP to Dell Networking W-Series Mobility Controller

W-IAP supports the configuration of tunneling protocols such as Generic Routing Encapsulation (GRE), IPsec, and L2TPv3. This section describes the procedure for configuring VPN host settings on a W-IAP to enable communication with a controller in a remote location:

- Configuring an IPSec Tunnel on page 210
- Enabling Automatic Configuration of GRE Tunnel on page 212
- Manually Configuring a GRE Tunnel on page 214
- Configuring an L2TPv3 Tunnel on page 215

Configuring an IPSec Tunnel

An IPsec tunnel is configured to ensure that the data flow between the networks is encrypted. When configured, the IPSec tunnel to the controller secures corporate data.

You can configure an IPSec tunnel from Virtual Controller using the Instant UI or CLI.

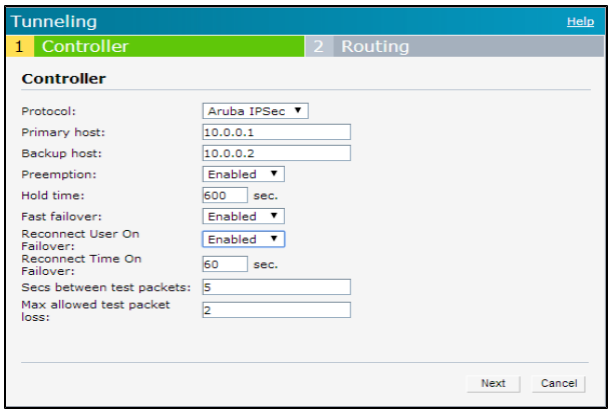
In the Instant UI

To configure a tunnel using the IPSec protocol:

1. Click the **More** > **VPN** link at the top right corner of the Instant UI. The **Tunneling** window is displayed.

2. Select **Aruba IPSec** from the **Protocol** drop-down list.
3. Enter the IP address or fully qualified domain name (FQDN) for the primary VPN/IPSec endpoint in the **Primary host** field.
4. Enter the IP address or FQDN for the backup VPN/IPSec endpoint in the **Backup host** field. This entry is optional. When you specify the primary and backup host details, the other fields are displayed.
5. Specify the following parameters. A sample configuration is shown in Figure 64.
   a. To allow the VPN tunnel to switch back to the primary host when it becomes available again, select **Enabled** from the **Preemption** drop-down list. This step is optional.
   b. If **Preemption** is enabled, specify a value in seconds for **Hold time**. When preemption is enabled and the primary host comes up, the VPN tunnel switches back to the primary host after the specified hold-time. The default value for **Hold time** is 600 seconds.
   c. To allow the W-IAP to create a backup VPN tunnel to the controller along with the primary tunnel, and maintain both the primary and backup tunnels separately, select **Enabled** from the **Fast failover** drop-down list. When fast failover is enabled and if the primary tunnel fails, the W-IAP can switch the data stream to the backup tunnel. This reduces the total failover time to less than one minute.
   d. To disconnect all wired and wireless users when the system switches during VPN tunnel transition from primary to backup and backup to primary, set **Reconnect user on failover** to **Enabled**.
   e. To configure an interval during which the wired and wireless users are disconnected during a VPN tunnel switch, specify a value in seconds for **Reconnect time on failover** within a range of 30–900 seconds. By default, the reconnection duration is set to 60 seconds.
   f. Specify a value in seconds for **Secs between test packets**. Based on the configured frequency, the W-IAP can verify if an active VPN connection is available. The default value is 5 seconds, which means that the W-IAP sends one packet to the controller every 5 seconds.
   g. Enter a value for **Max allowed test packet loss**, to define a number for lost packets, after which the W-IAP can determine that the VPN connection is unavailable. The default value is 2.

Figure 64 *IPSec Configuration*



6. Click **Next** to create routing profiles. When the IPsec tunnel configuration is completed, the packets that are sent from and received by a W-IAP are encrypted.

In the CLI

To configure an IPSec VPN tunnel:

```
(Instant AP)(config)# vpn primary <name>
(Instant AP)(config)# vpn backup <name>
(Instant AP)(config)# vpn fast-failover
(Instant AP)(config)# vpn hold-time <seconds>
(Instant AP)(config)# vpn preemption
(Instant AP)(config)# vpn monitor-pkt-send-freq <frequency>
```

```
(Instant AP)(config)# vpn monitor-pkt-lost-cnt <count>
(Instant AP)(config)# vpn reconnect-user-on-failover
(Instant AP)(config)# vpn reconnect-time-on-failover <down_time>
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Example

```
(Instant AP)(config)# vpn primary 192.0.2.18
(Instant AP)(config)# vpn backup 192.0.2.18
(Instant AP)(config)# vpn fast-failover
(Instant AP)(config)# vpn preemption

(Instant AP)(config)# ip dhcp distl2
(Instant AP)(DHCP Profile "distL2")# server-type Distributed,L2
(Instant AP)(DHCP Profile "distL2")# server-vlan 2
(Instant AP)(DHCP Profile "distL2")# ip-range 10.15.205.0 10.15.205.255
(Instant AP)(DHCP Profile "distL2")# subnet-mask 255.255.255.0
(Instant AP)(DHCP Profile "distL2")# lease-time 86400
(Instant AP)(DHCP Profile "distL2")# default-router 10.15.205.254
(Instant AP)(DHCP Profile "distL2")# dns-server 10.13.6.110,10.1.1.50
(Instant AP)(DHCP Profile "distL2")# domain-name dell.com
(Instant AP)(DHCP Profile "distL2")# client-count 5

(Instant AP)(config)# ip dhcp local
(Instant AP)(DHCP Profile "local")# server-type Local
(Instant AP)(DHCP Profile "local")# server-vlan 200
(Instant AP)(DHCP Profile "local")# subnet 172.16.200.1
(Instant AP)(DHCP Profile "local")# subnet-mask 255.255.255.0
(Instant AP)(DHCP Profile "local")# lease-time 86400
(Instant AP)(DHCP Profile "local")# dns-server 10.13.6.110,10.1.1.50
(Instant AP)(DHCP Profile "local")# domain-name dell.com
```

To view VPN configuration:

```
Instant Access Point# show vpn config
```

Enabling Automatic Configuration of GRE Tunnel

GRE is a tunnel protocol for encapsulating multicast, broadcast, and L2 packets between a controller and the W-IAPs. The automatic GRE feature uses the IPSec connection between the W-IAP and controller to send the control information for setting up a GRE tunnel. When automatic GRE configuration is enabled, a single IPSec tunnel between the W-IAP cluster and the controller and one or several GRE tunnels are created based on the Per-AP tunnel configuration on the W-IAP. When this feature is enabled on the W-IAP, no manual configuration is required on the controller to create the GRE tunnel.

Automatic configuration of the GRE tunnel is supported only on Dell controlleres. This feature is not supported on controllers running ArubaOS 6.3.x.x or lower versions.

You can configure a W-IAP to automatically set up a GRE tunnel from the W-IAP to Controller by using the Instant UI or CLI.

In the Instant UI

1. Click the **More** > **VPN** link at the top right corner of the Instant UI. The **Tunneling** window is displayed.
2. Select **Aruba GRE** from the **Protocol** drop-down list.
3. Enter the IP address or FQDN for the main VPN/IPSec endpoint in the **Primary host** field.
4. Enter the IP address or FQDN for the backup VPN/IPSec endpoint in the **Backup host** field. This entry is optional. When you enter the primary host IP address and backup host IP address, other fields are displayed.
5. Specify the following parameters. A sample configuration is shown in Figure 65.

a. To allow the VPN tunnel to switch back to the primary host when it becomes available again, select **Enabled** from the **Preemption** drop-down list. This step is optional.

b. If **Preemption** is enabled, specify a value in seconds for **Hold time**. When preemption is enabled and the primary host comes up, the VPN tunnel switches to the primary host after the specified hold time. The default value for **Hold time** is 600 seconds.

c. To allow the W-IAP to create a backup VPN tunnel to the controller along with the primary tunnel, and maintain both the primary and backup tunnels separately, select **Enabled** or **Disabled** from the **Fast failover** drop-down list. If the primary tunnel fails, the W-IAP can switch the data stream to the backup tunnel. This reduces the total failover time to less than one minute.

d. To disconnect all wired and wireless users when the system switches during VPN tunnel transition from primary to backup and backup to primary, set **Reconnect user on failover** to **Enabled**.

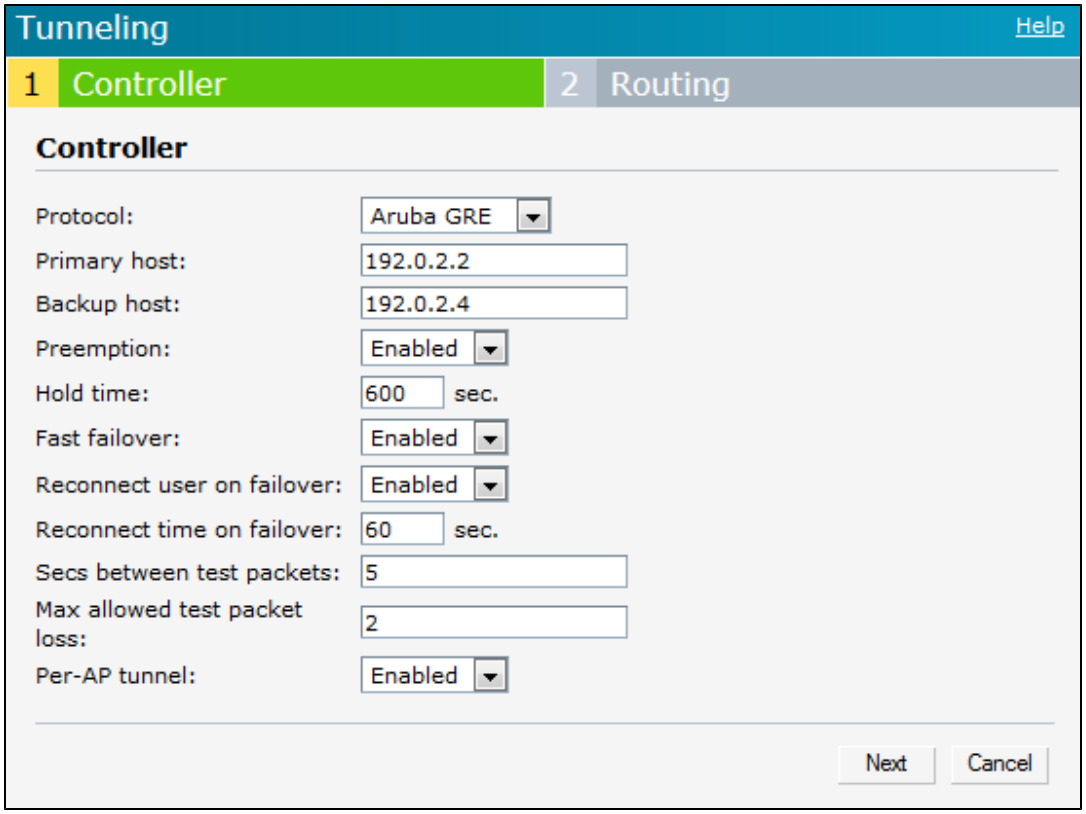
e. To configure an interval for which wired and wireless users are disconnected during a VPN tunnel switch, specify a value in seconds for **Reconnect time on failover** within the range of 30–900 seconds. By default, the reconnection duration is set to 60 seconds.

f. Specify a value in seconds for **Secs between test packets**. Based on the configured frequency, the W-IAP can verify if an active VPN connection is available. The default value is 5 seconds, which means that the W-IAP sends one packet to the controller every 5 seconds.

g. Enter a value for **Max allowed test packet loss**, to define a number for lost packets, after which the W-IAP can determine that the VPN connection is unavailable. The default value is 2.

h. Select **Enabled** or **Disabled** from the **Per-AP tunnel** drop-down list. The administrator can enable this option to create a GRE tunnel from each W-IAP to the VPN/GRE Endpoint rather than the tunnels created just from the master W-IAP. When enabled, the traffic to the corporate network is sent through a Layer-2 GRE tunnel from the W-IAP itself and need not be forwarded through the master W-IAP.

Figure 65 *Dell GRE Configuration*



6. Click **Next** to continue.

In the CLI

To enable automatic configuration of the GRE tunnel:

```
(Instant AP)(config)# vpn gre-outside
(Instant AP)(config)# vpn primary <name/IP-address>
(Instant AP)(config)# vpn backup <<name/IP-address>>
(Instant AP)(config)# vpn fast-failover
(Instant AP)(config)# vpn hold-time <seconds>
(Instant AP)(config)# vpn preemption
(Instant AP)(config)# vpn monitor-pkt-send-freq <frequency>
(Instant AP)(config)# vpn monitor-pkt-lost-cnt <count>
(Instant AP)(config)# vpn reconnect-user-on-failover
(Instant AP)(config)# vpn reconnect-time-on-failover <down_time>
(Instant AP)(config)# end
(Instant AP)# commit apply
```

To view VPN configuration details:

```
(Instant AP)# show vpn config
```

Manually Configuring a GRE Tunnel

You can also manually configure a GRE tunnel by configuring the GRE tunnel parameters on the W-IAP and controller. This procedure describes the steps involved in the manual configuration of a GRE tunnel from Virtual Controller by using the Instant UI or CLI.

During the manual GRE setup, you can either use the Virtual Controller IP or the W-IAP IP to create the GRE tunnel at the controller side depending upon the following W-IAP settings:

- If a Virtual Controller IP is configured and if Per-AP tunnel is disabled, the Virtual Controller IP is used to create the GRE tunnel.
- If a Virtual Controller IP is not configured or if Per-AP tunnel is enabled, the W-IAP IP is used to create the GRE tunnel.

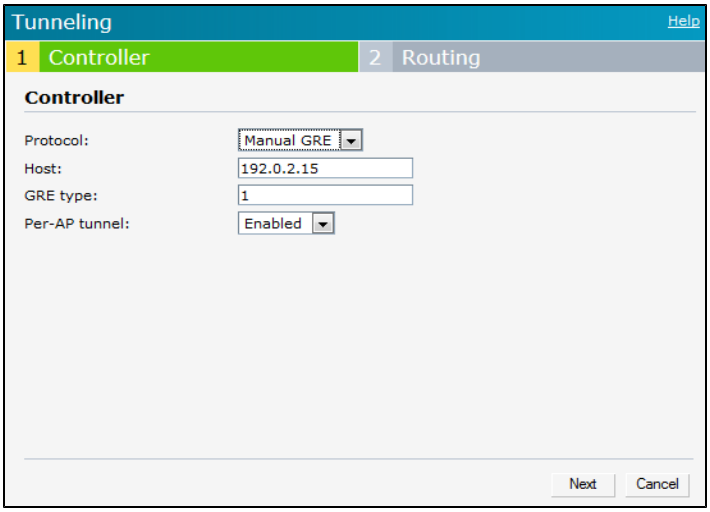
For information on the GRE tunnel configuration on controller, see *ArubaOS User Guide*.

In the Instant UI

1. Click the **More** > **VPN** link at the top right corner of the Instant UI. The **Tunneling** window is displayed.
2. Select **Manual GRE** from the **Protocol** drop-down list.
3. Specify the following parameters. A sample configuration is shown in Figure 66.
   a. Enter an IP address or the FQDN for the main VPN/GRE endpoint.
   b. Enter a value for the GRE type parameter.
   c. Select **Enabled** or **Disabled** from the **Per-AP tunnel** drop-down list. The administrator can enable this option to create a GRE tunnel from each W-IAP to the VPN/GRE Endpoint rather than the tunnels created just from the master W-IAP. When enabled, the traffic to the corporate network is sent through a Layer-2 GRE tunnel from the W-IAP itself and need not be forwarded through the master W-IAP.

By default, the **Per-AP tunnel** option is disabled.

Figure 66 *Manual GRE Configuration*



4. Click **Next** to continue. When the GRE tunnel configuration is completed on both the W-IAP and Controller, the packets sent from and received by a W-IAP are encapsulated, but not encrypted.

In the CLI

To configure a manual GRE VPN tunnel:

```
(Instant AP)(config)# gre primary <name>
(Instant AP)(config)# gre type <type>
(Instant AP)(config)# gre per-ap-tunnel
(Instant AP)(config)# end
(Instant AP)# commit apply
```

To view VPN configuration details:

```
Instant Access Point# show vpn config
```

To configure GRE tunnel on the controller:

```
(host)(config)# interface tunnel <Number>
(host)(config-tunnel)# description <Description>
(host)(config-tunnel)# tunnel mode gre <ID>
(host)(config-tunnel)# tunnel source <controller-IP>
(host)(config-tunnel)# tunnel destination <AP-IP>
(host)(config-tunnel)# trusted
(host)(config-tunnel)# tunnel vlan <allowed-VLAN>
```

Configuring an L2TPv3 Tunnel

The Layer 2 Tunneling Protocol version 3 (L2TPv3) feature allows W-IAP to act as L2TP Access Concentrator (LAC) and tunnel all wireless clients L2 traffic from AP to L2TP Network Server (LNS). In a centralized L2 model, the VLAN on the corporate side are extended to remote branch sites. Wireless clients associated with W-IAP gets the IP address from the DHCP server running on LNS. For this, AP has to transparently allow DHCP transactions through the L2TPv3 tunnel. In this release, L2TPv3 supports the following:

- Instant supports tunnel and session configuration, and uses Control Message Authentication (RFC 3931) for tunnel and session establishment. Each L2TPv3 tunnel supports one data connection and this connection is termed as an L2TPv3 session.
- Each W-IAP supports tunneling over UDP only.
- If the primary LNS is down, it fails over to the backup LNS. L2TPv3 has one tunnel profile and under this, one primary peer and a backup peer are configured. If the primary tunnel creation fails or if the primary tunnel gets deleted, the backup starts. The following two failover modes are supported:

- Preemptive: In this mode, if the primary comes up when the backup is active, the backup tunnel is deleted and the primary tunnel resumes as an active tunnel. If you configure the tunnel to be preemptive, and when the primary tunnel goes down, it starts the persistence timer which tries to bring up the primary tunnel.
- Non-Preemptive: In this mode, when the back tunnel is established after the primary tunnel goes down, it does not make the primary tunnel active again.

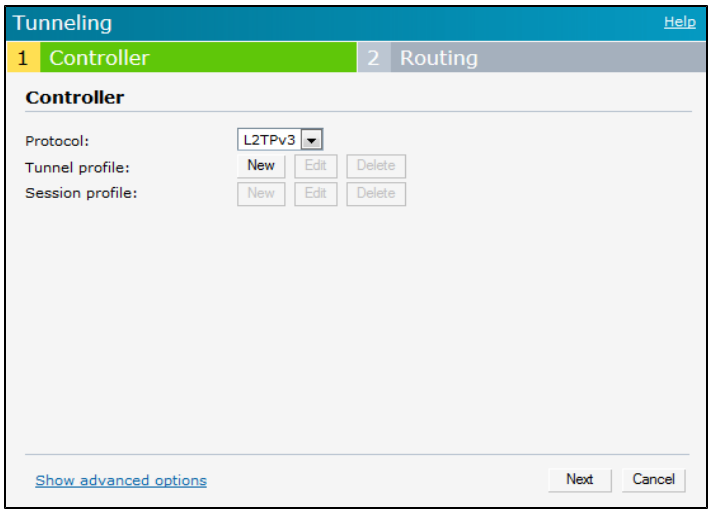
- L2TPV3 configuration is supported on the following W-IAPs:
  - W-IAP108
  - W-IAP109
  - W-IAP135

You can configure an L2TPv3 tunnel and session profiles through the Instant UI or CLI.

In the Instant UI

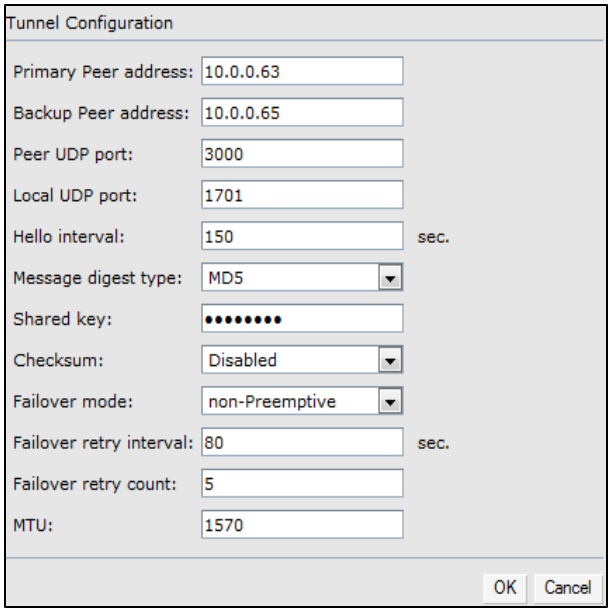
1. Click the **More** > **VPN** link at the top right corner of the Instant UI. The **Tunneling** window is displayed.

Figure 67 *L3TPv3 Tunneling*



2. Select **L2TPv3** from the Protocol drop-down list.
3. Configure the tunnel profile:
   a. Enter the tunnel name to be used for tunnel creation.

Figure 68 *Tunnel Configuration*



b. Enter the primary server IP address.

c. Enter the remote end backup tunnel IP address. This is an optional field and is required only when backup server is configured.

d. Enter the remote end UDP port number. The default value is 1701.

e. Enter the interval at which the hello packets are sent through the tunnel. The default value is 60 seconds.

f. Select the message digest as MD5 or SHA used for message authentication.

g. Enter a shared key for the message digest. This key should match with the tunnel end point shared key.

h. If required, select the failover mode as Primary or Backup (when the backup server is available).

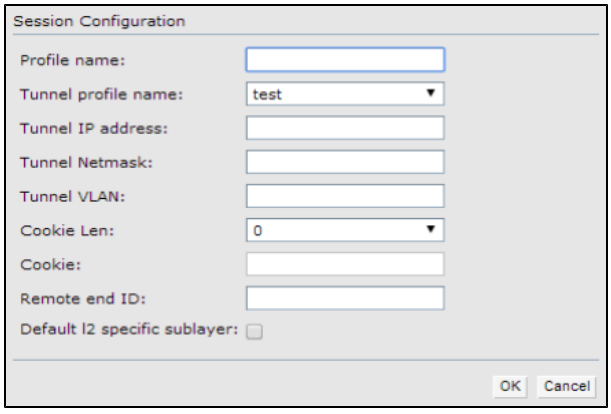
i. Specify a value for the tunnel MTU value if required. The default value is 1460.

j. Click **OK**.

4. Configure the session profile:

a. Enter the session name to be used for session creation.

Figure 69 *Session Configuration*



b. Enter the tunnel profile name where the session will be associated.

c. Configure the tunnel IP address with the corresponding network mask and VLAN ID. This is required to reach an AP from a corporate network. For example, SNMP polling.

d. Select the cookie length and enter a cookie value corresponding to the length. By default, the cookie length is not set.
e. Specify the remote end ID.
f. If required, enable default l2 specific sublayer in the L2TP session.
g. Click **OK**.

5. Click **Next** to continue.

In the CLI

To configure an L2TPv3 VPN tunnel profile:

```
(Instant AP)(config)# l2tpv3 tunnel <l2tpv3_tunnel_profile>
(Instant AP) (L2TPv3 Tunnel Profile <l2tpv3_tunnel_profile>)# primary peer-address <peer_ip_
addr_tunnel>
(Instant AP) (L2TPv3 Tunnel Profile <l2tpv3_tunnel_profile>)# backup peer-address <peer_ip_
addr_tunnel>
(Instant AP) (L2TPv3 Tunnel Profile <l2tpv3_tunnel_profile>)# checksum
(Instant AP) (L2TPv3 Tunnel Profile <l2tpv3_tunnel_profile>)# failover-mode <mode>
(Instant AP) (L2TPv3 Tunnel Profile <l2tpv3_tunnel_profile>)# failover-retry-count <retry_
count>
(Instant AP) (L2TPv3 Tunnel Profile <l2tpv3_tunnel_profile>)# failover-retry-interval
<interval_in_sec>
(Instant AP) (L2TPv3 Tunnel Profile <l2tpv3_tunnel_profile>)# hello-timeout <interval_in_sec>
(Instant AP) (L2TPv3 Tunnel Profile <l2tpv3_tunnel_profile>)# local-port <local_udp_port>
(Instant AP) (L2TPv3 Tunnel Profile <l2tpv3_tunnel_profile>)# peer-port <peer_udp_port>
(Instant AP) (L2TPv3 Tunnel Profile <l2tpv3_tunnel_profile>)# message-digest-type <digest_
algo>
(Instant AP) (L2TPv3 Tunnel Profile <l2tpv3_tunnel_profile>)# secret-key <key>
(Instant AP) (L2TPv3 Tunnel Profile <l2tpv3_tunnel_profile>)# mtu <tunnel_MTU>
(Instant AP) (L2TPv3 Tunnel Profile <l2tpv3_tunnel_profile>)# end
(Instant AP)# commit apply
```

To configure an L2TPv3 session profile:

```
(Instant AP)(config)# l2tpv3 session <l2tpv3_session_profile>
(Instant AP) (L2TPv3 Tunnel Profile <l2tpv3_session_profile>)# cookie len <len_of_cookie>
value <cookie_val>
(Instant AP) (L2TPv3 Tunnel Profile <l2tpv3_session_profile>)# l2tpv3 tunnel <l2tpv3_tunnel_
name_to_associate>
(Instant AP) (L2TPv3 Tunnel Profile <l2tpv3_session_profile>)# tunnel-ip <local_ip_addr_
tunnel> mask <tunnel_mask> vlan <tunnel_mgmt_vlan>
(Instant AP) (L2TPv3 Tunnel Profile <l2tpv3_session_profile>)# default-l2-specific-sublayer
(Instant AP) (L2TPv3 Tunnel Profile <l2tpv3_session_profile>)# end
(Instant AP)# commit apply
```

Example

```
(Instant AP)(config)# l2tpv3 tunnel test_tunnel
(Instant AP)(L2TPv3 Tunnel Profile "test_tunnel")# primary peer-address 10.0.0.65
(Instant AP)(L2TPv3 Tunnel Profile "test_tunnel")# backup peer-address 10.0.0.63
(Instant AP)(L2TPv3 Tunnel Profile "test_tunnel")# no checksum
(Instant AP)(L2TPv3 Tunnel Profile "test_tunnel")# failover-mode non-preemptive
(Instant AP)(L2TPv3 Tunnel Profile "test_tunnel")# failover-retry-count 5
(Instant AP)(L2TPv3 Tunnel Profile "test_tunnel")# failover-retry-interval 80
(Instant AP)(L2TPv3 Tunnel Profile "test_tunnel")# hello-timeout 150
(Instant AP)(L2TPv3 Tunnel Profile "test_tunnel")# mtu 1570
(Instant AP)(L2TPv3 Tunnel Profile "test_tunnel")# peer-port 3000
(Instant AP)(L2TPv3 Tunnel Profile "test_tunnel")# secret-key test123
(Instant AP)(L2TPv3 Tunnel Profile "test_tunnel")# end
(Instant AP) # commit apply
```

```
(Instant AP)(config) # l2tpv3 session test_session
(Instant AP)(L2TPv3 Session Profile "test_session")# cookie len 4 value 12345678
(Instant AP)(L2TPv3 Session Profile "test_session")# l2tpv3 tunnel test_tunnel
(Instant AP)(L2TPv3 Session Profile "test_session")# tunnel-ip 1.1.1.1 mask 255.255.255.0 vlan
5
(Instant AP)(L2TPv3 Tunnel Profile "test_tunnel")# end
(Instant AP)# commit apply
```

To view L2TPv3 configuration:

```
(Instant AP)# show l2tpv3 config
L2TPV3 Tunnel configuration
---------------------------
Tunnel Profile Primary Peer Backup Peer Peer UDP Port Local UDP Port Hello Interval Host Name
MTU Message Digest Type secret Key Failover Mode Failover Retry Count Retry Interval Checksum
-------------- ------------- ------------ ------------- -------------- -------------- --------
- --- -------------------- ---------- ------------- --------------------- -------------- -------
-
test_tunnel 10.0.0.63 10.0.0.65 3000 1701 150 Instant-C4:42:98 1570 MD5
625beed39fa4ff3424edb3082ede48fa non-preemptive 5 80 Disabled
L2TPV3 Session configuration
---------------------------
Session Name Tunnel Name Local tunnel IP Tunnel Mask Tunnel Vlan Session Cookie Length Session
Cookie Session Remote End ID
------------ ------------ ---------------- ------------ ------------ --------------------- -------
------- ----------------------
test_session 1.1.1.1 255.255.255.0 5 0 0 0
```

To view L2TPv3 global configuration:

```
(Instant AP)# show l2tpv3 global parameter

L2TPV3 Global configuration
---------------------------
Host Name
----------
Instant-C4:42:98
```

To view L2TPV3 session status:

```
(Instant AP)# show l2tpv3 session status

Session 1821009927 on tunnel 858508253:-
type: LAC Incoming Call, state: ESTABLISHED
created at: Jul 2 04:58:45 2013
administrative name: 'test_session' (primary)
created by admin: YES, peer session id: 12382
session profile name: test_session_primary
data sequencing required: OFF
use data sequence numbers: OFF
Peer configuration data:-
data sequencing required: OFF
framing types:
data rx packets: 16, rx bytes: 1560, rx errors: 0 rx cookie error 0
data tx packets: 6, tx bytes: 588, tx errors: 0
```

To view L2TPV3 tunnel status:

```
(Instant AP)# show l2tpv3 tunnel status

Tunnel 858508253, from 10.13.11.29 to 10.13.11.157:-
state: ESTABLISHED
created at: Jul 2 04:58:25 2013
```

```
administrative name: 'test_tunnel' (primary)
created by admin: YES, tunnel mode: LAC, persist: YES
local host name: Instant-C4:42:98
peer tunnel id: 1842732147, host name: aruba1600pop636635.hsbtst2.aus
UDP ports: local 1701, peer 3000
session limit: 0, session count: 1
tunnel profile: test_tunnel_primary, peer profile: default
session profile: default
hello timeout: 150, retry timeout: 80, idle timeout: 0
rx window size: 10, tx window size: 10, max retries: 5
use udp checksums: OFF
do pmtu discovery: OFF, mtu: 1460
trace flags: PROTOCOL FSM API AVPDATA FUNC XPRT DATA SYSTEM CLI
peer vendor name: Katalix Systems Ltd. Linux-2.6.32-358.2.1.el6.x86_64 (x86_64)
peer protocol version: 1.0, firmware 0
peer rx window size: 10
Transport status:-
ns/nr: 98/97, peer 98/96
cwnd: 10, ssthresh: 10, congpkt_acc: 9
Transport statistics:-
out-of-sequence control/data discards: 0/0
ACKs tx/txfail/rx: 0/0/96
retransmits: 0, duplicate pkt discards: 0, data pkt discards: 0
hellos tx/txfail/rx: 94/0/95
control rx packets: 193, rx bytes: 8506
control tx packets: 195, tx bytes: 8625
data rx packets: 0, rx bytes: 0, rx errors: 0
data tx packets: 6, tx bytes: 588, tx errors: 0
establish retries: 0
```

To view L2TPv3 tunnel config:

```
(Instant AP)# show l2tpv3 tunnel config

Tunnel profile test_tunnel_primary
l2tp host name: Instant-C4:42:98
local UDP port: 1701
peer IP address: 10.0.0.65
peer UDP port: 3000
hello timeout 150, retry timeout 80, idle timeout 0
rx window size 10, tx window size 10, max retries 5
use UDP checksums: OFF
do pmtu discovery: OFF, mtu: 1570
framing capability: SYNC ASYNC
bearer capability: DIGITAL ANALOG
use tiebreaker: OFF
peer profile: NOT SET
session profile: NOT SET
trace flags: PROTOCOL FSM API AVPDATA FUNC XPRT DATA SYSTEM CLI

Tunnel profile test_tunnel_backup
l2tp host name: aruba1600pop658509.hsb-dev4.aus
local UDP port: 1701
peer IP address: 10.13.11.157
peer UDP port: 1701
hello timeout 60, retry timeout 1, idle timeout 0
rx window size 10, tx window size 10, max retries 5
use UDP checksums: OFF
do pmtu discovery: OFF, mtu: 1460
framing capability: SYNC ASYNC
bearer capability: DIGITAL ANALOG
```

```
use tiebreaker: OFF
peer profile: NOT SET
session profile: NOT SET
trace flags: PROTOCOL FSM API AVPDATA FUNC XPRT DATA SYSTEM CLI
```

To view L2TPv3 system statistics:

```
(Instant AP)# show l2tpv3 system statistics

L2TP counters:-
Total messages sent: 99, received: 194, retransmitted: 0
illegal: 0, unsupported: 0, ignored AVPs: 0, vendor AVPs: 0
Setup failures: tunnels: 0, sessions: 0
Resource failures: control frames: 0, peers: 0
tunnels: 0, sessions: 0
Limit exceeded errors: tunnels: 0, sessions: 0
Frame errors: short frames: 0, wrong version frames: 0
unexpected data frames: 0, bad frames: 0
Internal: authentication failures: 0, message encode failures: 0
no matching tunnel discards: 0, mismatched tunnel ids: 0
no matching session_discards: 0, mismatched session ids: 0
total control frame send failures: 0, event queue fulls: 0
Message counters:-
Message RX Good RX Bad TX
ILLEGAL 0 0 0
SCCRQ 0 0 1
SCCRP 1 0 0
SCCCN 0 0 1
STOPCCN 0 0 0
RESERVED1 0 0 0
HELLO 95 0 95
OCRQ 0 0 0
OCRP 0 0 0
OCCN 0 0 0
ICRQ 0 0 1
ICRP 1 0 0
ICCN 0 0 1
RESERVED2 0 0 0
CDN 0 0 0
WEN 0 0 0
SLI 0 0 0
```

Configuring Routing Profiles

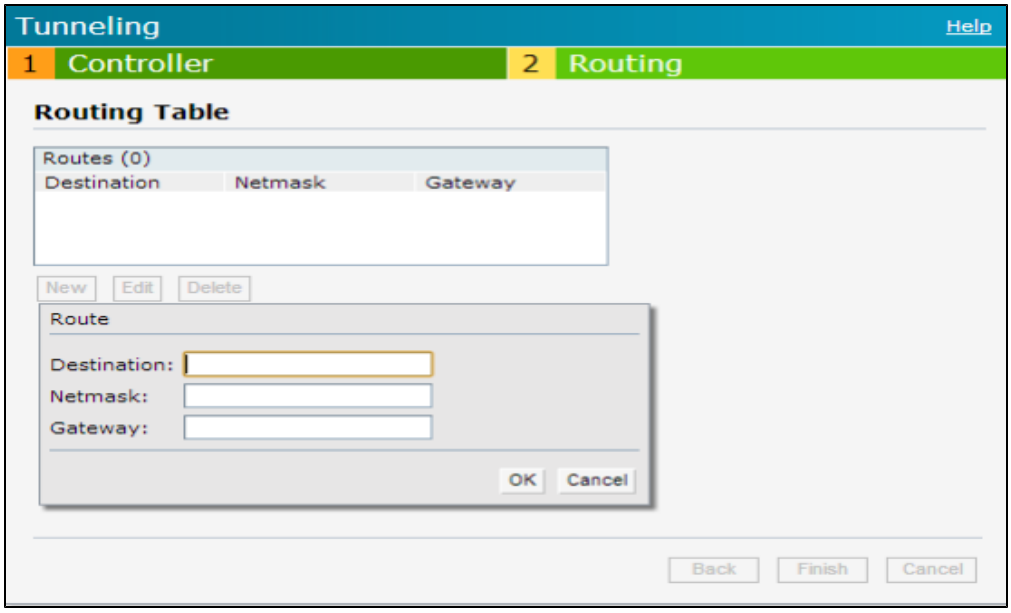
W-IAPs can terminate a single VPN connection on a Dell Networking W-Series mobility controller. The routing profile defines the corporate subnets which need to be tunneled through IPSec. You can configure routing profiles to specify a policy based on routing into the VPN tunnel using the Instant UI or CLI.

In the Instant UI

To configure a routing profile:

1. Click **Routing** in the **Tunneling** window. The routing details are displayed.
2. Click **New**. The route parameters to configure are displayed.

Figure 70 *Tunneling— Routing*



3. Update the following parameters:
   - **Destination**– Specify the destination network that is reachable through the VPN tunnel. This defines the IP or subnet that must reach through the IPsec tunnel. Traffic to the IP or subnet defined here will be forwarded through the IPsec tunnel.
   - **Netmask**– Specify the subnet mask to the destination defined for **Destination**.
   - **Gateway**– Specify the gateway to which traffic must be routed. This IP address must be the controller IP address on which the VPN connection is terminated. If you have a primary and backup host, configure two routes with the same destination and netmask, but ensure that the gateway is the primary controller IP for one route and the backup controller IP for the second route.
4. Repeat step 3 to create the required number of routing profiles.
5. Click **OK**.
6. Click **Finish**.

In the CLI

```
(Instant AP)(config)# routing-profile
(Instant AP)(Routing-profile)# route <destination> <mask> <gateway>
(Instant AP)(Routing-profile)# end
(Instant AP)# commit apply
```

This section provides the following information:

- Understanding IAP-VPN Architecture on page 223
- Configuring W-IAP and Controller for IAP-VPN Operations on page 225

Understanding IAP-VPN Architecture

The IAP-VPN architecture includes the following two components:

- W-IAPs at branch sites
- Controller at the datacenter

The master W-IAP at the branch acts as the VPN endpoint and the controller at the datacenter acts as the VPN concentrator. When a W-IAP is set up for VPN, it forms an IPsec tunnel to the controller to secure sensitive corporate data. IPsec authentication and authorization between the controller and the W-IAPs is based on the RAP whitelist configured on the controller.

Only the master AP in a W-IAP cluster forms the VPN tunnel.

From the controller perspective, the master W-IAPs that form the VPN tunnel are considered as VPN clients. The controller terminates VPN tunnels and routes or switches VPN traffic. The W-IAP cluster creates an IPSec or GRE VPN tunnel from the Virtual Controller to a mobility controller in a branch office. The controller only acts an IPSec or GRE VPN end-point and it does not configure the W-IAP.

IAP-VPN Scalability Limits

The controller scalability in IAP-VPN architecture depends on factors such as IPsec tunnel limit, Branch ID limit and datapath route table limit. The following table provides the IAP-VPN scalability information for various controller platforms:

Table 42: *IAP-VPN Scalability*

Platforms	Branches	Routes	L3 Mode Users	NAT Users	Total L2 Users
W-3200	1000	1000	N/A	N/A	64000
W-3400	2000	2000			64000
W-3600	8000	8000			64000
W-6000M3	8000	8000			64000
W-7210	8000	8000			64000
W-7220	16000	16000			128000
W-7240	32000	32000			128000

- **Branches**–The number of IAP-VPN branches that can be terminated on a given controller platform.
- **Routes**–The number of L3 routes supported on the controller.

- **L3 mode and NAT mode users**—The number of trusted users supported on the controller. There is no scale impact on the controller. They are limited only by the number of clients supported per W-IAP.
- **L2 mode users**—The number of L2 mode users are limited to 128000 for W-7220/W-7240 and 64000 across all platforms.

IAP-VPN Forwarding Modes

The following forwarding modes are supported in the IAP-VPN scenario.

- Local mode
- Centralized L2 mode
- Distributed L2 mode
- Distributed L3 mode

The forwarding modes determine whether the DHCP server and default gateway for clients reside in the branch or at the datacenter. These modes do not determine the firewall processing or traffic forwarding behavior. The Virtual Controller enables different DHCP pools (various assignment modes) in addition to allocating IP subnets for each branch. The Virtual Controller allows different modes of forwarding of traffic from the clients on a VLAN with a VPN tunnel. The forwarding modes are associated with various modes of DHCP address assignment modes.

Local or NAT Mode

In this mode, the W-IAP cluster at that branch has a local subnet and the master W-IAP of the cluster acts as the DHCP server and gateway for clients. The local mode provides VPN capabilities using the inner IP of the IAP-VPN IPsec tunnel. The source IP for all client traffic is translated and the traffic destined for the corporate network is translated using the VPN tunnel IP address of the W-IAP, and is forwarded through the IPsec VPN tunnel. The traffic destined for the non-corporate network is translated using the IP address of the IAP and is forwarded through the uplink.

When the local mode is used for forwarding client traffic, hosts on the corporate network cannot establish connections to the clients on the W-IAP, because the source address of the clients is translated.

L2 Switching Mode

In this mode, the traffic destined for the corporate network is bridged through the VPN tunnel to the controller. The traffic destined for the non-corporate network is translated using the IP address of the W-IAP and is forwarded through the uplink.

When a W-IAP registers with the controller, and is configured to use the L2 DHCP scope, the controller automatically adds the VPN tunnel associated to this W-IAP into the VLAN multicast table. This allows the clients connecting to the L2 mode VLAN to be part of the same L2 broadcast domain on the controller.

Distributed L2 Mode

In this mode, the W-IAP assigns an IP address from the configured subnet and forwards traffic to both corporate and non-corporate destinations. Clients receive the corporate IP with Virtual Controller as the DHCP server. The default gateway for the client still resides in the datacenter and hence this mode is an L2 extension of corporate VLAN to remote site. Either the controller or an upstream router can be the gateway for the clients. Client traffic destined to datacenter resources is forwarded by the Master AP (through the IPSec tunnel) to the client's default gateway in the datacenter.

Centralized L2 Mode

The centralized L2 mode extends the corporate VLAN or broadcast domain to remote branches. The DHCP server and the gateway for the clients reside in the datacenter. Either the controller or an upstream router can be the gateway for the clients. For DHCP services in centralized L2 mode, it is recommended that you use an external

DHCP server and not the DHCP server on the controller. Client traffic destined to datacenter resources is forwarded by the master W-IAP (through the IPsec tunnel) to the client's default gateway in the datacenter.

L3 Routing Mode

In this mode, the traffic destined for the corporate network is routed through the VPN tunnel to the controller. The traffic destined for the non-corporate network is translated using the IP address of the W-IAP and is forwarded through the uplink.

When a W-IAP registers with the controller and is configured to use the L3 DHCP scope, the Controller adds a route to enable the routing of traffic from the corporate network to clients on this subnet in the branch.

Distributed L3 mode

The distributed L3 mode contains all broadcast and multicast traffic to a branch. The distributed L3 mode reduces the cost and eliminates the complexity associated with the classic site-site VPN. However, this mode is very similar to a classic site-site IPsec VPN where two VPN endpoints connect individual networks together over a public network.

In distributed L3 mode, each branch location is assigned a dedicated subnet. The master AP in the branch manages the dedicated subnet and acts as the DHCP server and gateway for clients. Client traffic destined to datacenter resources is routed to the Dell controller through the IPsec tunnel which then routes the traffic to the appropriate corporate destinations.

Centralized L3 Mode

For centralized L3 clients, the virtual controller acts as a DHCP relay agent that forwards the DHCP traffic to the DHCP server located behind the controller in the corporate network and reachable through the IPSec tunnel. The centralized L3 VLAN IP is used as the source IP. The IP address is obtained from the DHCP server.

Configuring W-IAP and Controller for IAP-VPN Operations

This section describes the configuration procedures to perform on the W-IAP and controller for generic use cases. For information on specific deployment scenarios, see IAP-VPN Deployment Scenarios on page 356.

Configuring a W-IAP network for IAP-VPN operations

This section describes the configuration procedures to perform on the W-IAP for generic use cases. For information on specific deployment scenarios, see IAP-VPN Deployment Scenarios on page 356.

A W-IAP network requires the following configuration for IAP-VPN operations.

1. Defining the VPN host settings
2. Configuring Routing Profiles
3. Configuring DHCP Profiles
4. Configuring an SSID or Wired Port
5. Enabling Dynamic RADIUS Proxy
6. Configuring Enterprise Domains

Defining the VPN host settings

The VPN endpoint on which a master W-IAP terminates its VPN tunnel is considered as the host. A master AP in a W-IAP network can be configured with a primary and backup host to provide VPN redundancy. You can define VPN host settings through **More**>**VPN**>**Controller** in the UI.

You can configure the following VPN profiles for the IAP-VPN operations. For more information, see Configuring a Tunnel from a W-IAP to Dell Networking W-Series Mobility Controller on page 210.

- IPSec
- Aruba GRE
- Manual GRE

Configuring Routing Profiles

The routing profile on the W-IAP determines whether the traffic destined to a subnet must be tunneled through IPSec or bridged locally. If the routing profile is empty, the client traffic will always be bridged locally. For example, if the routing profile is configured to tunnel 10.0.0.0 /8, traffic destined to 10.0.0.0 /8 will be forwarded through the IPsec tunnel and the traffic to all other destinations is bridged locally.

You can also configure a routing profile with 0.0.0.0 as gateway to allow both client and IAP traffic to be routed through a non-tunnel route. If the gateway is in the same subnet as uplink IP address, it is used as a static gateway entry. A static route can be added on all master and slave W-IAPs for these destinations. The VPN traffic from the local subnet of W-IAP or the virtual controller IP address in the local subnet is not routed to tunnel, but will be switched to the relevant VLAN. For example, when a 0.0.0.0/0.0.0.0 routing profile is defined, to bypass certain IPs, you can add a route to the IP by defining 0.0.0.0 as the destination, thereby forcing the traffic to be routed through the default gateway of the W-IAP.

You can configure routing profiles through **More**>**VPN**>**Controller** UI. For step-by-step procedural information on configuring routing profile, see Configuring Routing Profiles on page 221.

The W-IAP network has only one active tunnel even when fast failover enabled. At any given time, traffic can be tunneled only to one VPN host.

Configuring DHCP Profiles

You can create DHCP profiles to determine the IAP-VPN mode of operation. A W-IAP network can have multiple DHCP profiles configured for different modes of IAP-VPN. You can configure up to eight DHCP profiles. For more information on the IAP-VPN modes of operation, see IAP-VPN Forwarding Modes on page 224.

You can create any of the following types of DHCP profiles for the IAP-VPN operations:

- Local
- Local L3
- Distributed L2
- Distributed L3
- Centralized

For more information on configuring DHCP profiles, see Configuring DHCP Scopes on page 201..

A centralized L2 or distributed L2 VLAN or subnet cannot be used to serve APs in a hierarchical mode of deployment. Ensure that the physical IP of the APs connecting to the master AP in hierarchical mode of deployment is not on a VLAN or subnet that is in centralized or distributed L2 mode of operation. For information on hierarchical mode of deployment, see Understanding Hierarchical Deployment on page 119.

Configuring an SSID or Wired Port

For a client to connect to the IAP-VPN network, an SSID or wired port profile on a W-IAP must be configured with appropriate IAP-VPN mode of operation. The VLAN configuration in an SSID or wired port profile determines whether an SSID or wired port is configured for the IAP-VPN operations.

To configure an SSID or wired port for a specific IAP-VPN mode, the VLAN ID defined in the SSID or wired port profile must match the VLAN ID defined in the DHCP profile configuration. If the VLAN assignment for an SSID or wired port profile is set to Virtual controller assigned, default, or a static VLAN ID that does not match the VLAN ID

configured in the DHCP profiles, the IAP-VPN operations are affected. For example, if a local DHCP profile is configured with a VLAN ID of 200, the VLAN configuration on the SSID must be set to a static VLAN ID 200.

For information on how to configure an SSID or wired port profile, seeWireless Network Profiles on page 93 and Configuring a Wired Profile on page 112 respectively.

Enabling Dynamic RADIUS Proxy

The RADIUS server can be deployed at different locations and VLANs. In most cases, a centralized RADIUS or local server is used to authenticate users. However, some user networks can use a local RADIUS server for employee authentication and a centralized RADIUS based captive portal server for guest authentication. To ensure that the RADIUS traffic is routed to the required RADIUS server, the dynamic RADIUS proxy feature must be enabled. When enabled, dynamic RADIUS proxy ensures that all the RADIUS traffic is sourced from the Virtual Controller IP or inner IP of the W-IAP IPsec tunnel depending on the RADIUS server IP and routing profile.

Ensure that a static Virtual Controller IP is configured before enabling dynamic RADIUS proxy, in order to tunnel the RADIUS traffic to the central RADIUS server in the datacenter.

For information on enabling dynamic RADIUS proxy, see Configuring Dynamic RADIUS Proxy Parameters on page 161.

Configuring Enterprise Domains

By default, all the DNS requests from a client are forwarded to the clients DNS server. In a typical W-IAP deployment without VPN configuration, client DNS requests are resolved by the DNS server of clients. For the IAP-VPN scenario, the enterprise domain settings on the W-IAP are used for determining how client DNS requests are routed. For information on how to configure enterprise domains, see Configuring Enterprise Domains on page 188.

Configuring a Controller for IAP-VPN Operations

Dell Networking W-Series controllers provide an ability to terminate the IPSec and GRE VPN tunnels from the W-IAP and provide corporate connectivity to the branch network. For IAP-VPN operations, ensure that the following configuration and verification procedures are completed on the controller:

- OSPF Configuration
- VPN Configuration
- Branch-ID Allocation
- Branch Status Verification

This section describes the configuration procedures to perform on the controller for generic use cases. For information on specific deployment scenarios, see IAP-VPN Deployment Scenarios on page 356.

ArubaOS 6.3 or later is the recommended version to run on the controllers for the IAP-VPN configuration. The IAP-VPN configuration is not supported on W-600 Series controllers.

OSPF Configuration

Open Shortest Path First (OSPF) is a dynamic Interior Gateway routing Protocol (IGP) based on IETF RFC 2328. The premise of OSPF is that the shortest or fastest routing path is used. The implementation of OSPFv2 allows controllers to deploy effectively in a Layer 3 topology. The controllers can act as the default gateway for all clients and forward user packets to the upstream router.

Each IAP-VPN can be defined a separate subnet derived from the corporate intranet pool to allow IAP-VPN devices to work independently. For sample topology and configuration, see *ArubaOS User Guide*.

To redistribute IAP-VPN routes into the OSPF process, use the following command :

```
(host)(config) # router ospf redistribute rapng-vpn
```

To verify if the redistribution of the IAP-VPN is enabled, use following command:

```
(host) #show ip ospf redistribute
Redistribute RAPNG
```

To configure aggregate route for IAP-VPN routes, use the following command:

```
(host) (config) # router ospf aggregate-route rapng-vpn
```

To view the aggregated routes for IAP-VPN routes, use the following command:

```
(host) #show ip ospf rapng-vpn aggregate-routes
RAPNG VPN aggregate routes
--------------------------
Prefix Mask Contributing routes Cost
------ ---- ------------------ ----
201.201.200.0 255.255.252.0 5 268779624
100.100.2.0 255.255.255.0 1 10
```

To verify the details of configured aggregated route, use the following command:

```
(host) # show ip ospf rapng-vpn aggregated-routes <net> <mask>
(host) #show ip ospf rapng-vpn aggregate-routes 100.100.2.0 255.255.255.0
Contributing routes of RAPNG VPN aggregate route
------------------------------------------------
Prefix Mask Next-Hop Cost
------ ---- -------- ----
100.100.2.64 255.255.255.224 5.5.0.10 10
```

To view all the redistributed routes:

```
(host) #show ip ospf database
OSPF Database Table
-------------------
Area ID LSA Type Link ID Adv Router Age Seq# Checksum
------- -------- ------- ---------- --- ---- --------
0.0.0.15 ROUTER 9.9.9.9 9.9.9.9 159 0x80000016 0xee92
0.0.0.15 ROUTER 10.15.148.12 10.15.148.12 166 0x80000016 0x4c0d
0.0.0.15 NETWORK 10.15.148.12 10.15.148.12 167 0x80000001 0x9674
0.0.0.15 NSSA 12.12.2.0 9.9.9.9 29 0x80000003 0x7b54
0.0.0.15 NSSA 12.12.12.0 9.9.9.9 164 0x80000008 0x63a
0.0.0.15 NSSA 12.12.12.32 9.9.9.9 164 0x80000008 0x7b8
0.0.0.15 NSSA 50.40.40.0 9.9.9.9 164 0x80000007 0x8ed4
0.0.0.15 NSSA 51.41.41.128 9.9.9.9 164 0x80000007 0x68f6
0.0.0.15 NSSA 53.43.43.32 9.9.9.9 164 0x80000007 0x2633
0.0.0.15 NSSA 54.44.44.16 9.9.9.9 164 0x80000007 0x353
N/A AS_EXTERNAL 12.12.2.0 9.9.9.9 29 0x80000003 0x8c06
N/A AS_EXTERNAL 12.12.12.0 9.9.9.9 169 0x80000001 0x25e4
N/A AS_EXTERNAL 12.12.12.32 9.9.9.9 169 0x80000001 0x2663
N/A AS_EXTERNAL 50.40.40.0 9.9.9.9 169 0x80000001 0xab80
N/A AS_EXTERNAL 51.41.41.128 9.9.9.9 169 0x80000001 0x85a2
N/A AS_EXTERNAL 53.43.43.32 9.9.9.9 169 0x80000001 0x43de
N/A AS_EXTERNAL 54.44.44.16 9.9.9.9 169 0x80000001 0x20fe
```

To verify if the redistributed routes are installed or not:

```
(host) #show ip route
Codes: C - connected, O - OSPF, R - RIP, S - static
M - mgmt, U - route usable, * - candidate default, V - RAPNG VPN
Gateway of last resort is Imported from DHCP to network 0.0.0.0 at cost 10
Gateway of last resort is Imported from CELL to network 0.0.0.0 at cost 10
Gateway of last resort is Imported from PPPOE to network 0.0.0.0 at cost 10
Gateway of last resort is 10.15.148.254 to network 0.0.0.0 at cost 1
S* 0.0.0.0/0 [1/0] via 10.15.148.254*
```

```
V 12.12.2.0/24 [10/0] ipsec map
V 12.12.12.0/25 [10/0] ipsec map
V 12.12.12.32/27 [10/0] ipsec map
V 50.40.40.0/24 [10/0] ipsec map
V 51.41.41.128/25 [10/0] ipsec map
V 53.43.43.32/27 [10/0] ipsec map
V 54.44.44.16/28 [10/0] ipsec map
C 9.9.9.0/24 is directly connected, VLAN9
C 10.15.148.0/24 is directly connected, VLAN1
C 43.43.43.0/24 is directly connected, VLAN132
C 42.42.42.0/24 is directly connected, VLAN123
C 44.44.44.0/24 is directly connected, VLAN125
C 182.82.82.12/32 is an ipsec map 10.15.149.69-182.82.82.12
C 182.82.82.14/32 is an ipsec map 10.17.87.126-182.82.82.14
```

VPN Configuration

The following VPN configuration steps on the controller enable the W-IAPs to terminate their VPN connection on the controller:

Whitelist Database Configuration

The whitelist database is a list of the MAC addresses of the W-IAPs that are allowed to establish VPN connections with the controller. This list can be either stored in the controller database or on an external server.

You can use the following CLI command to configure the whitelist database entry if the controller is acting as the whitelist database:

```
(host)# whitelist-db rap add mac-address 00:11:22:33:44:55 ap-group test
```

The **ap-group** parameter is not used for any configuration, but needs to be configured. The parameter can be any valid string.

If an external server is used as the location for the whitelist database, add the MAC addresses of the valid W-IAPs in the external database or external directory server and then configure a RADIUS server to authenticate the W-IAPs using the entries in the external database or external directory server.

If you are using the Windows 2003 server, perform the following steps to configure the external whitelist database on it. There are equivalent steps available for the Windows Server 2008 and other RADIUS servers.

1. Add the MAC addresses for all the W-IAPs in the Active Directory of the RADIUS server:
   a. Open the **Active Directory and Computers** window, add a new user and specify the MAC address (without the colon delimiter) of the W-IAP for the user name and password.
   b. Right-click the user that you have just created and click **Properties**.
   c. In the **Dial-in** tab, select **Allow access** in the **Remote Access Permission** section and click **OK**.
   d. Repeat Step a through Step b for all W-IAPs.
2. Define the remote access policy in the Internet Authentication Service:
   a. In the **Internet Authentication Service** window, select **Remote Access Policies**.
   b. Launch the wizard to configure a new remote access policy.
   c. Define filters and select **grant remote access permission** in the **Permissions** window.
   d. Right-click the policy that you have just created and select **Properties**.
   e. In the **Settings** tab, select the policy condition, and **Edit Profile...**.
   f. In the **Advanced** tab, select **Vendor Specific**, and click **Add** to add new vendor specific attributes.
   g. Add new vendor specific attributes and click **OK**.
   h. In the **IP** tab, provide the IP address of the W-IAP and click **OK**.

VPN Local Pool Configuration

The VPN local pool is used to assign an IP Address to the W-IAP after successful XAUTH VPN.

```
(host) # ip local pool "rapngpool" <startip> <endip>
```

Role Assignment for the Authenticated W-IAPs

Define a role that includes a src-nat rule to allow connections to the RADIUS server and for the Dynamic Radius Proxy in the W-IAP to work. This role is assigned to W-IAPs after successful authentication.

```
(host) (config) #ip access-list session iaprole
(host) (config-sess-iaprole)#any host <radius-server-ip> any src-nat
(host) (config-sess-iaprole)#any any any permit
(host) (config-sess-iaprole)#!
(host) (config) #user-role iaprole
(host) (config-role) #session-acl iaprole
```

VPN Profile Configuration

The VPN profile configuration defines the server used to authenticate the W-IAP (internal or an external server) and the role assigned to the IAP after successful authentication.

```
(host) (config) #aaa authentication vpn default-iap
(host) (VPN Authentication Profile "default-iap") #server-group default
(host) (VPN Authentication Profile "default-iap") #default-role iaprole
```

Branch-ID Allocation

For branches deployed in distributed L3 and distributed L2 mode, the master AP in the branch and the controller should agree upon a subnet/IP addresses to be used for DHCP services in the branch. The process or protocol used by the master AP and the controller to determine the subnet/IP addresses used in a branch is called BID allocation. The BID allocation process is not essential for branches deployed in local or centralized L2 mode. The following are some of the key functions of the BID allocation process:

- Determines the IP addresses used in a branch for distributed L2 mode
- Determines the subnet used in a branch for distributed L3 mode
- Avoids IP address or subnet overlap (that is, avoids IP conflict)
- Ensures that a branch is allocated the same subnet or range of IP addresses irrespective of which AP in the branch becomes the master in the IAP cluster

Branch Status Verification

To view the details of the branch information connected to the controller, execute the **show iap table** command.

Example

This example shows the details of the branches connected to the controller:

```
(host) #show iap table long

IAP Branch Table
----------------
Name VC MAC Address Status Inner IP Assigned Subnet Assigned Vlan
---- -------------- ------ -------- --------------- -------------
Tokyo-CB:D3:16 6c:f3:7f:cc:42:f8 DOWN 0.0.0.0
Paris-CB:D3:16 6c:f3:7f:cc:3d:04 UP 10.15.207.140 10.15.206.99/29 2
LA 6c:f3:7f:cc:42:25 UP 10.15.207.111 10.15.206.24/29 2
Munich d8:c7:c8:cb:d3:16 DOWN 0.0.0.0
London-c0:e1 6c:f3:7f:c0:e1:b1 UP 10.15.207.120 10.15.206.64/29 2
Instant-CB:D3 6c:f3:7f:cc:42:1e DOWN 0.0.0.0
Delhi 6c:f3:7f:cc:42:ca DOWN 0.0.0.0
Singapore 6c:f3:7f:cc:42:cb UP 10.15.207.122 10.15.206.120/29 2
```

```
Key Bid(Subnet Name)
--- ----------------
b3c65c...
b3c65c...
b3c65c... 2(10.15.205.0-10.15.205.250,5),1(10.15.206.1-10.15.206.252,5)
a2a65c... 0
b3c65c... 7(10.15.205.0-10.15.205.250,5),8(10.15.206.1-10.15.206.252,5)
b3c65c...
b3c65c... 1(10.15.205.0-10.15.205.250,5),2(10.15.206.1-10.15.206.252,5)
b3c65c... 14(10.15.205.0-10.15.205.250,5),15(10.15.206.1-10.15.206.252,5)
```

The output of this command provides the following information:

Table 43: *Branch Details*

Parameter	Description
`Name`	Displays the name of the branch.
`VC MAC Address`	Displays the MAC address of the Virtual Controller of the branch.
`Status`	Displays the current status of the branch (UP/DOWN).
`Inner IP`	Displays the internal VPN IP of the branch.
`Assigned Subnet`	Displays the subnet mask assigned to the branch.
`Assigned Vlan`	Displays the VLAN ID assigned to the branch.
`Key`	Displays the key for the branch, which is unique to each branch.
`Bid(Subnet Name)`	Displays the Branch ID (BID) of the subnet. • In the example above, the controller displays bid-per-subnet-per-branch i.e., for "LA" branch, BID "2" for the ip-range "10.15.205.0-10.15.205.250" with client count per branch "5"). If a branch has multiple subnets, it can have multiple BIDs. • If a branch is in **UP** state and does not have a **Bid(Subnet Name)**, it means that the W-IAP is connected to a controller, which did not assign any BID for any subnet. In the above example, "Paris-CB:D3:16" branch is **UP** and does not have a **Bid (Subnet Name)**. This means that either the W-IAP is connected to a backup controller or it is connected to a primary controller without any distributed L2 or L3 subnets.

The **show iap table** command output does not display the **Key** and **Bid(Subnet Name)** details.

This chapter provides the following information:

- ARM Overview on page 232
- Configuring ARM Features on a W-IAP on page 233
- Configuring Radio Settings for a W-IAP on page 238

ARM Overview

Adaptive Radio Management (ARM) is a radio frequency management technology that optimizes WLAN performance even in the networks with highest traffic by dynamically and intelligently choosing the best 802.11 channel and transmitting power for each W-IAP in its current RF environment. ARM works with all standard clients, across all operating systems, while remaining in compliance with the IEEE 802.11 standards. It does not require any proprietary client software to achieve its performance goals. ARM ensures low-latency roaming, consistently high performance, and maximum client compatibility in a multi-channel environment. By ensuring the fair distribution of available Wi-Fi bandwidth to mobile devices, ARM ensures that data, voice, and video applications have sufficient network resources at all times. ARM allows mixed 802.11a, b, g, n, and ac client types to inter operate at the highest performance levels.

Channel or Power Assignment

The channel or power assignment feature automatically assigns channel and power settings for all the W-IAPs in the network according to changes in the RF environment. This feature automates many setup tasks during network installation and the ongoing operations when RF conditions change.

Voice Aware Scanning

The Voice Aware scanning feature prevents a W-IAP supporting an active voice call from scanning for other channels in the RF spectrum and allows a W-IAP to resume scanning when there are no active voice calls. This significantly improves the voice quality when a call is in progress and simultaneously delivers the automated RF management functions. By default, this feature is enabled.

Load Aware Scanning

The Load Aware Scanning feature dynamically adjusts scanning behavior to maintain uninterrupted data transfer on resource intensive systems when the network traffic exceeds a predefined threshold. The W-IAPs resume complete monitoring scans when the traffic drops to the normal levels. By default, this feature is enabled.

Monitoring the Network with ARM

When ARM is enabled, a W-IAP dynamically scans all 802.11 channels within its 802.11 regulatory domain at regular intervals and sends reports to a Virtual Controller on network (WLAN) coverage, interference, and intrusion detection.

ARM Metrics

ARM computes coverage and interference metrics for each valid channel and chooses the best performing channel and transmit power settings for each W-IAP RF environment. Each W-IAP gathers other metrics on its ARM-assigned channel to provide a snapshot of the current RF health state.

Configuring ARM Features on a W-IAP

This section describes the following procedures for configuring ARM features:

- Band Steering on page 233
- Airtime Fairness Mode on page 233
- Client Match on page 234
- Access Point Control on page 236

Band Steering

The band steering feature assigns the dual-band capable clients to the 5 GHz band on dual-band W-IAPs. This feature reduces co-channel interference and increases available bandwidth for dual-band clients, because there are more channels on the 5 GHz band than on the 2.4 GHz band. You can configure band steering parameters through the Instant UI or CLI.

In the Instant UI

To configure band steering:

1. In the **RF** > **ARM** >**Show advanced options** view, configure the following parameters:

Table 44: *Band Steering Mode - Configuration Parameters*

Parameter	Description
Prefer 5 GHz	Select this option to use band steering in the 5 GHz mode. On selecting this, the W-IAP steers the client to the 5 GHz band (if the client is 5 GHz capable), but allows the client connection on the 2.4 GHz band if the client persistently attempts for 2.4 GHz association.
Force 5 GHz	Select this option to enforce 5 GHz band steering mode on the W-IAPs.
Balance Bands	Select this option to allow the W-IAP to balance the clients across the two radios to best utilize the available 2.4 GHz bandwidth. This feature takes into account the fact that the 5 GHz band has more channels than the 2.4 GHz band, and that the 5 GHz channels operate in 40MHz, while the 2.5 GHz band operates in 20MHz.
Disabled	Select this option if you want to allow the clients to select the band to use.

2. Click **OK**.

In the CLI

To configure band steering:

```
(Instant AP)(config)# arm
(Instant AP)(ARM)# band-steering-mode {<Prefer 5 GHz>| <Force 5 GHz>|<Balance
Bands>|<Disabled>}
(Instant AP)(ARM)# end
(Instant AP)# commit apply
```

Airtime Fairness Mode

The airtime fairness feature provides equal access to all clients on the wireless medium, regardless of client type, capability, or operating system, thus delivering uniform performance to all clients. This feature prevents the clients from monopolizing resources. You can configure airtime fairness mode parameters through the Instant UI or CLI.

In the Instant UI

1. For **Airtime fairness mode** configuration, specify any of the following values in the **RF** > **ARM** >**Show advanced options** tab:

Table 45: *Airtime Fairness Mode - Configuration Parameters*

Parameter	Description
Default Access	Select this option to provide access based on client requests. When **Air Time Fairness** is set to default access, per user and per SSID bandwidth limits are not enforced.
Fair Access	Select this option to allocate Airtime evenly across all the clients.
Preferred Access	Select this option to set a preference where 11n clients are assigned more airtime than 11a/11g. The 11a/11g clients get more airtime than 11b. The ratio is 16:4:1.

2. Click **OK**.

In the CLI

```
(Instant AP)(config)# arm
(Instant AP)(ARM)# air-time-fairness-mode {<Default Access>| <Fair Access> | <Preferred Access>
(Instant AP)(ARM)# end
(Instant AP)# commit apply
```

Client Match

The ARM client match feature continually monitors a client's RF neighborhood to provide ongoing client band steering and load balancing, and enhanced AP reassignment for roaming mobile clients. This feature supersedes the legacy band steering and spectrum load balancing features, which, unlike client match, do not trigger W-IAP changes for clients already associated to a W-IAP.

Legacy 802.11a/b/g access points do not support the client match feature. When client match is enabled on 802.11n capable access points, the client match feature overrides any settings configured for the legacy band steering, station hand off assist or load balancing features. 802.11ac-capable access points do not support the legacy band steering, station hand off or load balancing settings, so these access points must be managed using client match.

When the client match feature is enabled on a W-IAP, the W-IAP measures the RF health of its associated clients. In the current release, the client match feature is supported only within a W-IAP cluster. If any of the following trigger conditions is met, clients are moved from one AP to another for better performance and client experience:

- **Dynamic Load Balancing**: Client match balances clients across W-IAPs on different channels, based on the client load on the W-IAPs and the SNR levels the client detects from an underutilized W-IAP. If a W-IAP radio can support additional clients, the W-IAP will participate in client match load balancing and clients can be directed to that W-IAP radio, subject to the predefined SNR thresholds. For better load balancing, clients are steered from busy channels to idle channels.
- **Sticky Clients**: The client match feature also helps mobile clients that tend to stay associated to a W-IAP despite low signal levels. W-IAPs using client match continually monitor the client's RSSI as it roams between W-IAPs, and move the client to a W-IAP when a better radio match can be found. This prevents mobile clients from remaining associated to an APs with less than ideal RSSI, which can cause poor connectivity and reduce performance for other clients associated with that W-IAP.

- **Band Steering**: W-IAPs using the client match feature monitor the RSSI for clients that advertise a dual-band capability. If a client is currently associated to a 2.4 GHz radio and the AP detects that the client has a good RSSI from the 5 GHz radio, the W-IAP steers the client to the 5 GHz radio, as long as the 5 GHz RSSI is not significantly worse than the 2.4 GHz RSSI, and the W-IAP retains a suitable distribution of clients on each of its radios.
- **Channel Utilization**: Based on the percentage of channel utilization, clients are steered from a busy channel to an idle channel.
- **Client Capability Match**: Based on the client capability match, clients are steered to appropriate channel, for example, HT20, HT40, or VHT80.

In the Instant 6.3.1.1-4.0 release, spectrum load balancing is integrated with the client match feature. Client match allows the APs in a cluster to be divided into several logical AP RF neighborhood called domains, which share the same clients. The Virtual Controller determines the distribution of clients and balances client load across channels, regardless of whether the AP is responding to the probe requests of wireless clients.

You can configure client match parameters in Instant UI or CLI. When client match is enabled, the dashboard in the main window displays the **Client Match** link on selecting an AP in the **Access Points** tab or a client in the **Clients** tab. Clicking this link provides a graphical representation of radio map view of an AP and the client distribution on an AP radio. For more information, see Client Match on page 66.

In the Instant UI

1. For client match configuration, specify the following parameters the **RF** > **ARM** >**Show advanced options** tab:

Table 46: *Client Match Configuration Parameters*

Parameter	Description
Client match	Select **Enabled** to enable the **Client match** feature on APs. When enabled, client count will be balanced among all the channels in the same band. For more information, see ARM Overview on page 232. By default, the client match feature is disabled. **NOTE:** When client match is enabled, ensure that Scanning is enabled.
CM calculating interval	Specify a value for the calculating interval of Client match. The value specified for **CM calculating interval** determines the interval at which client match is calculated. The interval is specified in seconds and the default value is 30 seconds. You can specify a value within the range of 10-600.
CM neighbor matching %	Specify a value for **CM neighbor matching %**. This number takes into account the least similarity percentage to be considered as in the same virtual RF neighborhood of client match. You can specify a percentage value within the range of 20-100. The default value is 75%.
CM threshold	Specify a value for **CM threshold**. This number takes acceptance client count difference among all the channels of Client match into account. When the client load on an AP reaches or exceeds the threshold in comparison, client match is enabled on that AP. You can specify a value within range of 1-255. The default value is 2.
SLB mode	Select a mode from the **SLB mode** drop-down list. The SLB mode determines the balancing strategy for client match. The following options are available: • Channel • Radio • Channel + Radio

2. Click **OK**.

In the CLI

```
(Instant AP)(config)# arm
(Instant AP)(ARM)# client-match calc-interval <seconds>
(Instant AP)(ARM)# client-match calc-threshold <threshold>
(Instant AP)(ARM)# client-match nb-matching <percentage>
(Instant AP)(ARM)# client-match slb-mode 1
(Instant AP)(ARM)# end
(Instant AP)# commit apply
```

Access Point Control

You can configure access point control parameters through the Instant UI or CLI.

In the Instant UI

1. For **Access Point Control**, specify the following parameters in the **RF** > **ARM** >**Show advanced options** tab:

Table 47: *Access Point Control - Configuration Parameters*

Parameter	Description
Customize Valid Channels	Select this checkbox to customize valid channels for 2,4 GHz and 5 GHz. By default, the AP uses valid channels as defined by the Country Code (regulatory domain). On selecting the **Customize Valid Channels** checkbox, a list of valid channels for both 2.4.GHz and 5 GHz are displayed. The valid channel customization feature is disabled by default..
Minimum Transmit Power	Specify the minimum transmission power. The value specified for **Minimum Transmit Power** indicates the minimum Effective Isotropic Radiated Power (EIRP) from 3 to 33 dBm in 3 dBm increments. If the minimum transmission EIRP setting configured on an AP is not supported by the AP model, this value is reduced to the highest supported power setting. The default value is for minimum transmit power is 18 dBm.
Maximum Transmit Power	Specify the maximum transmission power. The value specified for **Maximum Transmit Power** indicates the maximum Effective Isotropic Radiated Power (EIRP) from 3 to 33 dBm in 3 dBm increments. If the maximum transmission EIRP configured on an AP is not supported by the AP model, the value is reduced to the highest supported power setting. The default value for maximum transmit power is 127 dBm.
Client aware	When **Enabled**, ARM does not change channels for the APs with active clients, except for high priority events such as radar or excessive noise. This feature must be enabled in most deployments for a stable WLAN. If the Client Aware mode is **Disabled**, the W-IAP may change to a more optimal channel, which change may disrupt current client traffic for a while. The Client aware option is **Enabled** by default. **NOTE:** When Client aware is disabled, channels can be changed even when the clients are active on a BSSID.

Parameter	Description
Scanning	Select **Enabled** so that the W-IAP dynamically scans all 802.11 channels within its 802.11 regulatory domain at regular intervals and reports to the W-IAP. This scanning report includes WLAN coverage, interference, and intrusion detection data. **NOTE:** For client match configuration, ensure that scanning is enabled.
Wide Channel Bands	Select a band to allow the APs to be placed in 40Mhz (wide band) channels. The **Wide channel band** allows administrators to configure 40 MHz channels in the 2.4 GHz and 5.0 GHz bands. 40 MHz channels are two 20 MHz adjacent channels that are bonded together. 40 MHz channel effectively doubles the frequency bandwidth available for data transmission.
80 MHz Support	Enables or disables the use of 80 MHz channels on APs. This feature allows ARM to assign 80 MHz channels on APs with 5GHz radios, which support a very high throughput. This setting is enabled by default. **NOTE:** Only the APs that support 802.11ac can be configured with 80 MHz channels.

2. Reboot the W-IAP.
3. Click **OK**.

In the CLI

To configure access point control parameters:

```
(Instant AP)(config)# arm
(Instant AP)(ARM)# a-channels <5GHz-channels>
(Instant AP)(ARM)# min-tx-power <power>
(Instant AP)(ARM)# max-tx-power <power>
(Instant AP)(ARM)# client-aware
(Instant AP)(ARM)# wide-bands {<5GHz>|<2GHz>|<All>|<None>}
(Instant AP)(ARM)# scanning
(Instant AP)(ARM)# 80mhz-support
(Instant AP)(ARM)# end
(Instant AP)# commit apply
```

Verifying ARM Configuration

To view ARM configuration:

```
(Instant AP)# show arm config

Minimum Transmit Power :18
Maximum Transmit Power :127
Band Steering Mode :prefer-5ghz
Client Aware :enable
Scanning :enable
Wide Channel Bands :5ghz
80Mhz Support :enable
Air Time Fairness Mode :fair-access
Client Match :disable
CM NB Matching Percent :75
CM Calculating Interval :30
CM SLB Threshold :2
CM SLB Balancing Mode :channel based
CM max client match req :5
CM max adoption :5
Custom Channels :No
2.4 GHz Channels
```

```
----------------
Channel Status
------- ------
1 enable
2 disable
3 disable
4 disable
5 disable
6 enable
7 disable
8 disable
9 disable
10 disable
11 enable
12 disable
13 disable
1+ enable
2+ disable
3+ disable
4+ disable
5+ disable
6+ disable
7+ enable
5.0 GHz Channels
----------------
Channel Status
------- ------
36 enable
40 enable
44 enable
48 enable
52 enable
56 enable
60 enable
64 enable
149 enable
153 enable
157 enable
161 enable
165 enable
36+ enable
44+ enable
52+ disable
60+ disable
149+ enable
157+ enable
36E enable
52E enable
149E enable
```

Configuring Radio Settings for a W-IAP

You can configure 2.4 GHz and 5 GHz radio settings for a W-IAP either using the Instant UI or CLI.

In the Instant UI

To configure radio settings:

1. Click the **RF** link at the top right corner of the Instant main window.
2. Click **Show advanced options**. The advanced options are displayed.

3. Click the **Radio** tab.
4. Under the channel 2.4.GHz or 5GHz or both, configure the following parameters.

Table 48: *Radio Configuration Parameters*

Parameter	Description
Legacy only	Select **Enabled** to run the radio in non-802.11n mode. This option is set to **Disabled** by default.
802.11d / 802.11h	Select **Enabled** to allow the radio to advertise its 802.11d (Country Information) and 802.11h (Transmit Power Control) capabilities. This option is set to **Disabled** by default.
Beacon interval	Enter the Beacon period for the W-IAP in milliseconds. This indicates how often the 802.11 beacon management frames are transmitted by the access point. You can specify a value within the range of 60-500. The default value is 100 milliseconds.
Interference immunity level	Select to increase the immunity level to improve performance in high-interference environments. The default immunity level is 2. • **Level 0**– no ANI adaptation. • **Level 1**– Noise immunity only. This level enables power-based packet detection by controlling the amount of power increase that makes a radio aware that it has received a packet. • **Level 2**– Noise and spur immunity. This level also controls the detection of OFDM packets, and is the default setting for the Noise Immunity feature. • **Level 3**– Level 2 settings and weak OFDM immunity. This level minimizes false detects on the radio due to interference, but may also reduce radio sensitivity. This level is recommended for environments with a high-level of interference related to 2.4 GHz appliances such as cordless phones. • **Level 4**– Level 3 settings, and FIR immunity. At this level, the AP adjusts its sensitivity to in-band power, which can improve performance in environments with high and constant levels of noise interference. • **Level 5**– The AP completely disables PHY error reporting, improving performance by eliminating the time the W-IAP would spend on PHY processing. **NOTE:** Increasing the immunity level makes the AP to lose a small amount of range.
Channel switch announcement count	Specify the count to indicate the number of channel switching announcements that must be sent before switching to a new channel. This allows associated clients to recover gracefully from a channel change.
Background spectrum monitoring	Select **Enabled** to allow the APs in access mode to continue with normal access service to clients, while performing additional function of monitoring RF interference (from both neighboring APs and non Wi-Fi sources such as, microwaves and cordless phones) on the channel they are currently serving clients.

5. Reboot the W-IAP after configuring the radio profile settings.

In the CLI

To configure 2.4 GHz radio settings:

```
(Instant AP)(config)# rf dot11g-radio-profile
(Instant AP)(RF dot11 g Radio Profile)# beacon-interval <milliseconds>
(Instant AP)(RF dot11 g Radio Profile)# legacy-mode
(Instant AP)(RF dot11 g Radio Profile)# spectrum-monitor
(Instant AP)(RF dot11 g Radio Profile)# dot11h
(Instant AP)(RF dot11 g Radio Profile)# interference-immunity <level>
(Instant AP)(RF dot11 g Radio Profile)# csa-count <count>
(Instant AP)(RF dot11 g Radio Profile)# max-distance <count>
(Instant AP)(RF dot11 g Radio Profile)# end
```

```
(Instant AP)# commit apply
```

To configure 5 GHz radio settings:

```
(Instant AP)(config)# rf dot11a-radio-profile
(Instant AP)(RF dot11a Radio Profile)# beacon-interval <milliseconds>
(Instant AP)(RF dot11a Radio Profile)# legacy-mode
(Instant AP)(RF dot11a Radio Profile)# spectrum-monitor
(Instant AP)(RF dot11a Radio Profile)# spectrum-band <type>
(Instant AP)(RF dot11a Radio Profile)# dot11h
(Instant AP)(RF dot11a Radio Profile)# interference-immunity <level>
(Instant AP)(RF dot11a Radio Profile)# max-distance <count>
(Instant AP)(RF dot11a Radio Profile)# csa-count <count>
(Instant AP)(RF dot11 g Radio Profile)# end
(Instant AP)# commit apply
```

To view the radio configuration:

```
(Instant AP)# show radio config

Legacy Mode:enable
Beacon Interval:100
802.11d/802.11h:enable
Interference Immunity Level:2
Channel Switch Announcement Count:0
MAX Distance:600
Channel Reuse Type:disable
Channel Reuse Threshold:0
Background Spectrum Monitor:disable

5.0 GHz:
Legacy Mode:enable
Beacon Interval:100
802.11d/802.11h:enable
Interference Immunity Level:2
Channel Switch Announcement Count:2
MAX Distance:600
Channel Reuse Type:disable
Channel Reuse Threshold:0
Background Spectrum Monitor:disable
Standalone Spectrum Band:5ghz-upper
```

This chapter provides the following information:

- Deep Packet Inspection on page 241
- Enabling Application Visibility on page 241
- Application Visibility on page 242
- Configuring Access Rules for Application and Application Categories on page 246
- Configuring Web Policy Enforcement on page 249

Deep Packet Inspection

AppRF is Dell's custom built Layer 7 firewall capability. It comprises of an on-board deep packet inspection and a cloud-based Web Policy Enforcement service that allows creating firewall policies based on types of application. The web policy enforcement capabilities require the W-IAP to have a web policy enforcement subscription. Please contact the Dell Sales Team.

W-IAPs with DPI capability analyze data packets to identify applications in-use and allow you to create access rules to determine client access to applications, application categories, web categories and website URLs based on security ratings. You can also define traffic shaping policies such as bandwidth control and QoS per application for client roles. For example, you can block bandwidth monopolizing applications on a guest role within an enterprise.

The AppRF feature provides application visibility for analyzing client traffic flow. W-IAPs support both the power of in-device packet flow identification and dynamically updated cloud-based web categorization.

To view the graphs, set the **AppRF visibility** option in the **System** window to **Enabled**. For more information on DPI ACLs and AppRF visibility, see the following topics:

Enabling Application Visibility

Enabling AppRF visibility allows you to view the AppRF statistics for a W-IAP or the clients associated with a W-IAP. When visibility is enabled, the AppRF link appears on the dashboard area of the main window. On clicking this link, you can view the client traffic flow based on the enforcements.

You can enable AppRF visibility through the Instant UI or CLI:

In the Instant UI

1. Navigate to **System**>**General**.
2. Select Enabled from the **AppRF visibility** drop-down.
3. Click **OK**.

In the CLI

To enable AppRF visibility:

```
(Instant AP)(config)# dpi
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Application Visibility

The AppRF graphs are based on Deep Packet Inspection (DPI) application and Web Policy Enforcement service, which provides application traffic summary for the client devices associated with a W-IAP. The **AppRF** link above the activity panel of the dashboard is displayed only if **AppRF visibility** is enabled in the **System** window.

The following figure provides a view of the AppRF dashboard:

Figure 71 *AppRF Dashboard*

The AppRF dashboard presents four different graph areas with data graphs on all client traffic and content filters based on web category and security ratings. Click on each category to view real-time client traffic data or usage trend in the last 15 minutes.

NOTE

The application charts are not supported on W-IAP104/105, W-IAP134/135, W-IAP175P/175AC, and W-IAP3WN/3WNP platforms. Only the web category charts are displayed for these W-IAP models.

Application Category Charts

The application category chart displays details on the client traffic towards the application categories. On clicking in the rectangle area, you can view the following graphs and toggle between the chart and list views.

Figure 72 *Application Categories Chart - Client View*

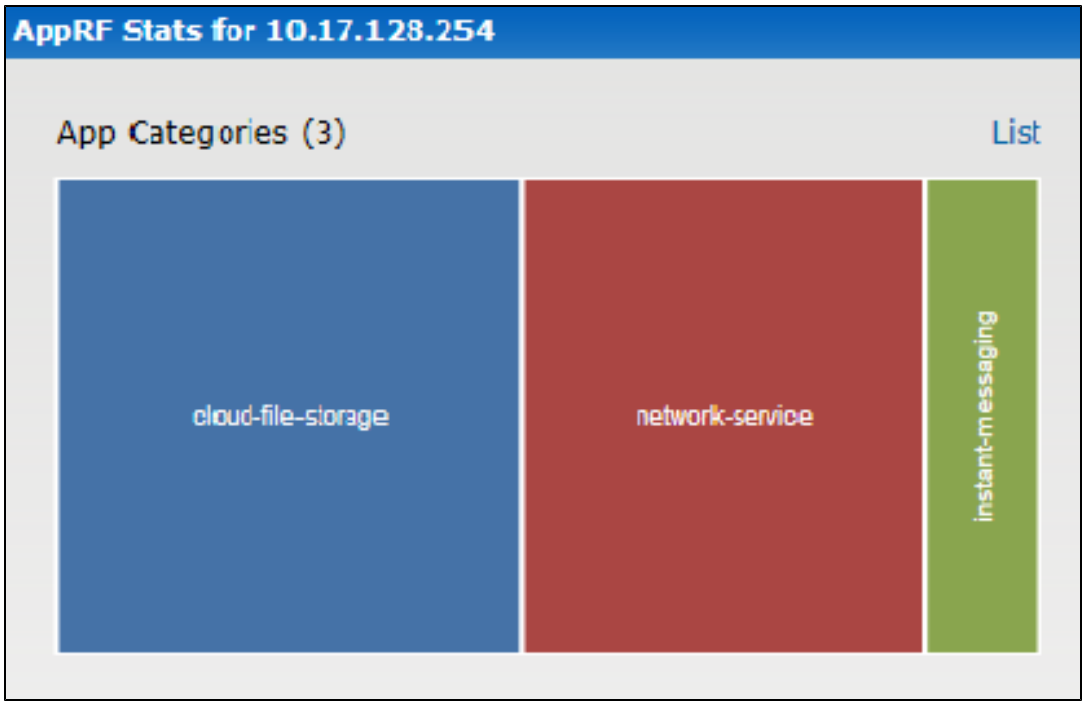


Figure 73 *Application Categories List - Client View*

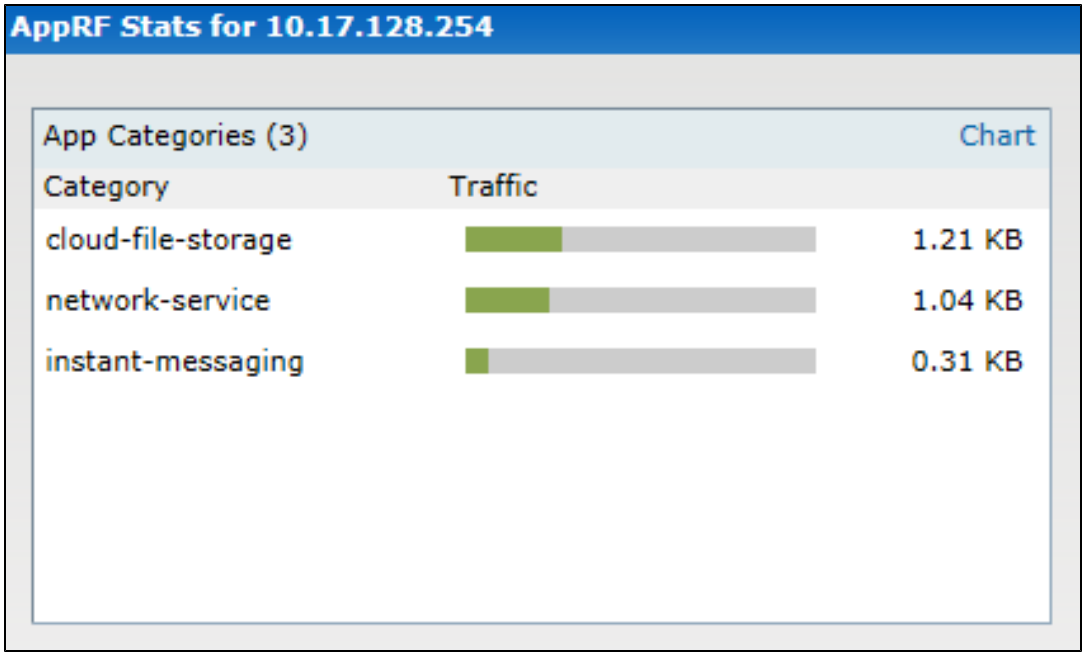
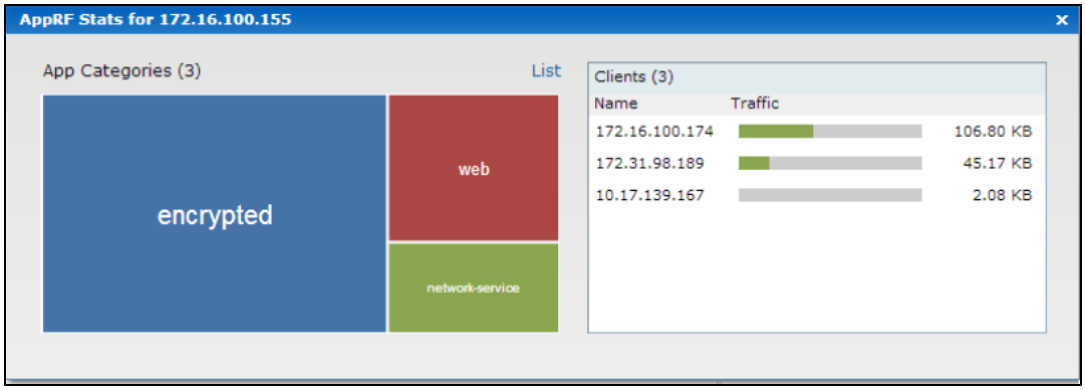


Figure 74 *Application Category Chart - AP View*



Application Charts

The application chart displays details on the client traffic towards the applications. On clicking in the rectangle area, you can view the following graphs and toggle between the chart and list views.

Figure 75 *Application Chart - Client View*

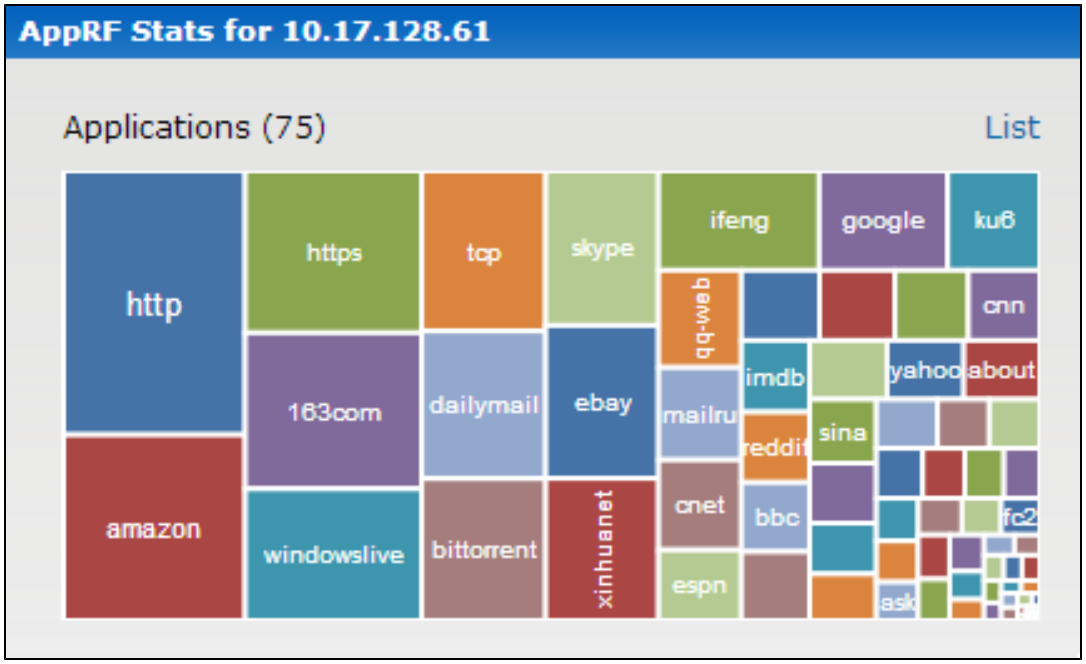


Figure 76 *Application List - Client View*

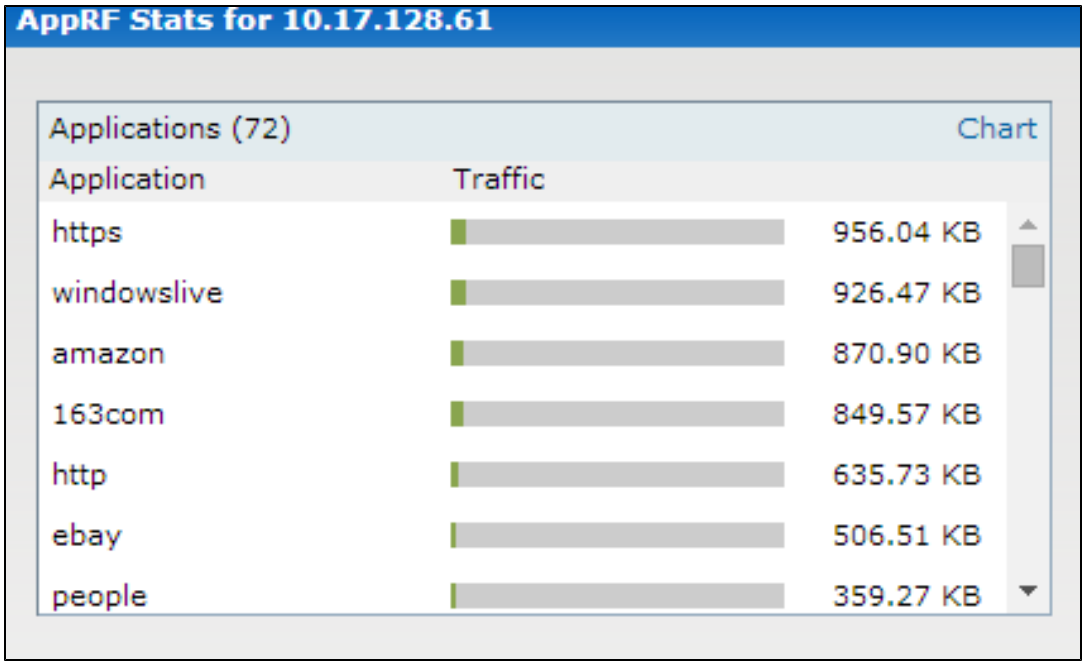
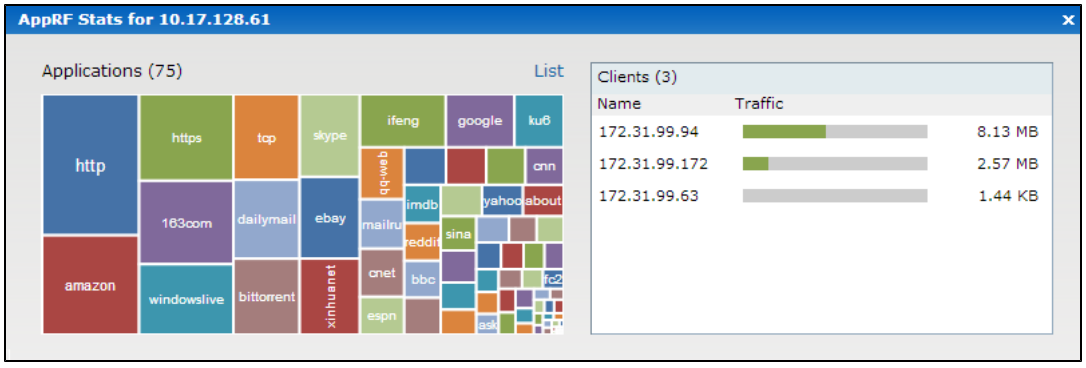


Figure 77 *Application Chart - AP View*



Web Categories Charts

The web categories chart displays details about the client traffic to the web categories. On clicking in the rectangle area, you can view the following graphs and toggle between the chart and list views.

Figure 78 *Web Categories Chart - Client View*

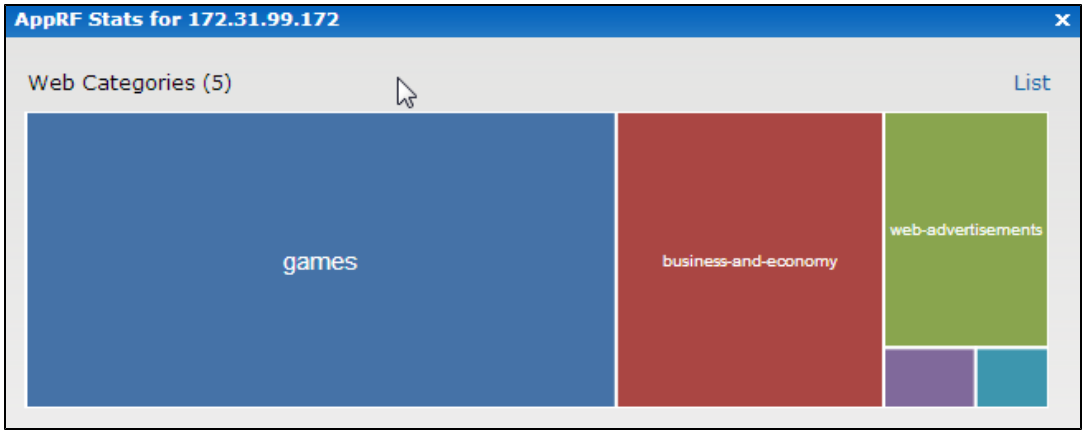


Figure 79 *Web Categories List - Client View*

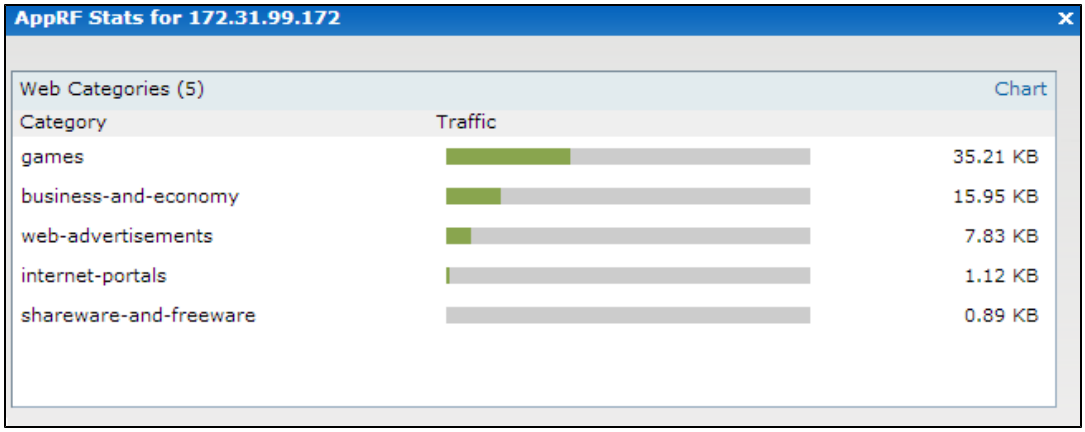
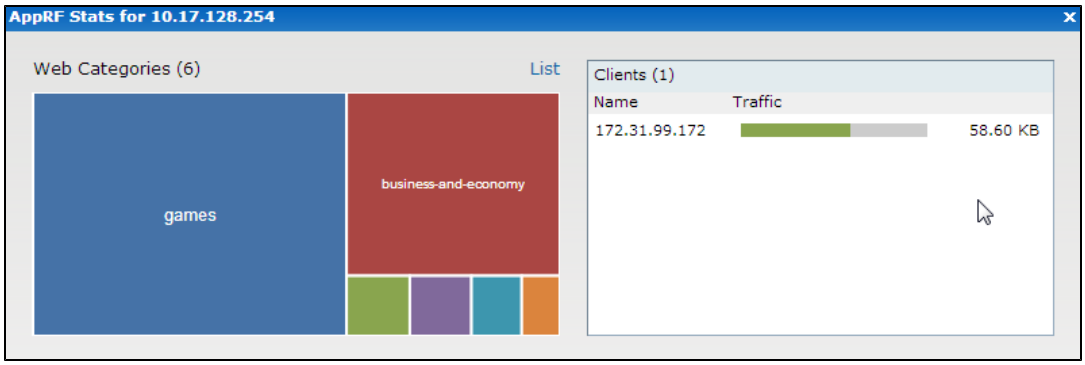


Figure 80 *Web Categories Chart - AP View*



Web Reputation Charts

The web reputation chart displays details about the client traffic to the URLs with that are assigned a security score. On clicking in the rectangle area, you can view the following graphs and toggle between the chart and list views.

Figure 81 *Web Reputation Chart - Client View*

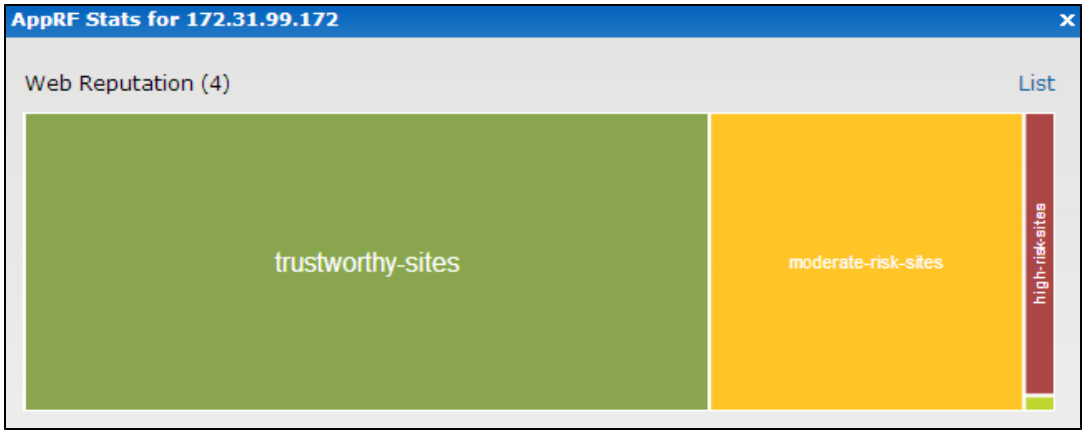


Figure 82 *Web Reputation List - Client View*

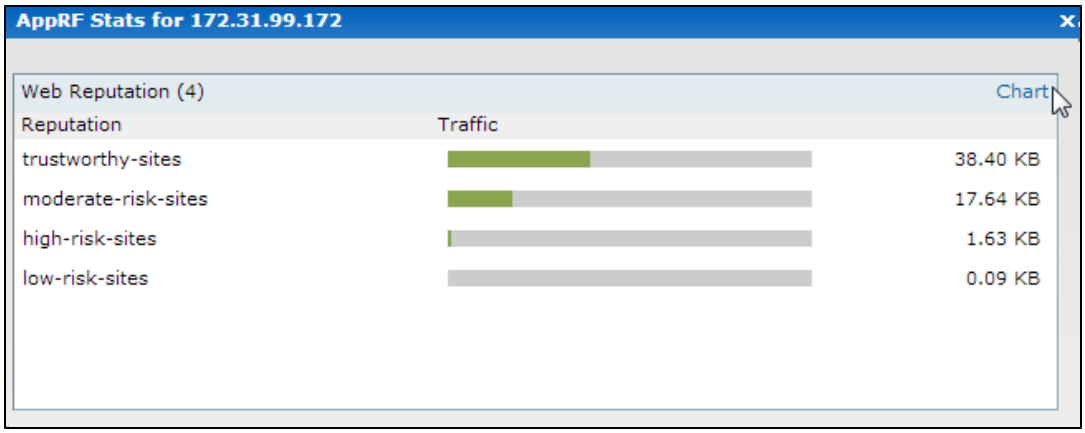
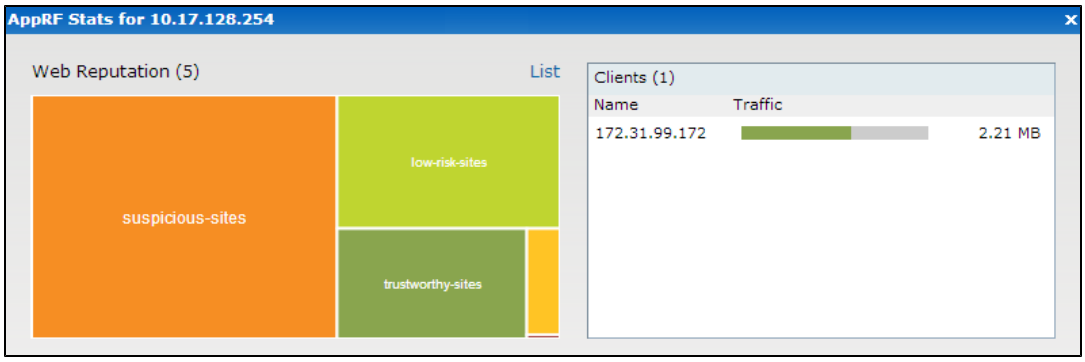


Figure 83 *Web Reputation Chart - AP View*



Configuring Access Rules for Application and Application Categories

This section describes the procedure for configuring access rules based on application and application categories. The Application and Application rules utilize the on-board DPI engine. For information on:

- Configuring access rules to control access to network services, see Configuring Access Rules for Network Services on page 177.
- Configuring access rules based on web categories and web reputation, see Configuring Web Policy Enforcement on page 249

In the Instant UI

To configure ACL rules for a user role:

1. Navigate to **Security** > **Roles** tab. The **Roles** tab contents are displayed.

   You can also configure access rules for a wired or wireless client through the WLAN wizard (**Network** tab>**WLAN SSID**> **Edit**>**Edit WLAN** > **Access**) or the Wired profile (**More** > **Wired**>**Edit**> **Edit Wired Network**> **Access**) window.
2. Select the role for which you want to configure access rules.
3. In **Access rules** section, click **New** to add a new rule. The **New Rule** window is displayed.
4. Ensure that the rule type is set to **Access Control**
5. To configure access to applications or application category, select a service category from the following list:
   - Application
   - Application category

Configuring access rules based on application and application category is not supported on W-IAP104/105, W-IAP134/135, and W-IAP3WN/3WNP platforms.

6. Based on the selected service category, configure the following parameters:

Table 49: *Access Rule Configuration Parameters*

Service Category	Description
Application	Select the applications to which you want to allow or deny access.
Application category	Select any of the following application categories to which you want to allow or deny access: • antivirus • authentication • cloud-file-storage • collaboration • encrypted • enterprise-apps • gaming • im-file-transfer • instant-messaging • mail-protocols • mobile-app-store • network-service • peer-to-peer • social-networking • standard • streaming • thin-client • tunneling • unified-communications • web • Webmail
Application Throttling	Application throttling allows you to set a bandwidth limit for an application, application category, web category, or for sites based on their web reputation. For example, you can limit the bandwidth rate for video streaming applications such as Youtube or Netflix, or assign a low bandwidth to high risk sites. If your W-IAP model does not support configuring access rules based on application or application category, you can create a rule based on web category or website reputation and assign bandwidth rates. To specify a bandwidth limit:

Table 49: *Access Rule Configuration Parameters*

Service Category	Description
	1. Select the **Application Throttling** checkbox. 2. Specify the downstream and upstream rates in Kbps.
Action	Select any of following actions: • Select **Allow** to allow access users based on the access rule. • Select **Deny** to deny access to users based on the access rule. • Select **Destination-NAT** to allow changes to destination IP address. • Select **Source-NAT** to allow changes to the source IP address. The destination-nat and source-nat actions apply only to the network services rules.
Destination	Select a destination option for the access rules for network services, applications, and application categories. You can allow or deny access to any the following destinations based on your requirements. • **to all destinations**– Access is allowed or denied to all destinations. • **to a particular server**–Access is allowed or denied to a particular server. After selecting this option, specify the IP address of the destination server. • **except to a particular server**–Access is allowed or denied to servers other than the specified server. After selecting this option, specify the IP address of the destination server. • **to a network**–Access is allowed or denied to a network. After selecting this option, specify the IP address and netmask for the destination network. • **except to a network**–Access is allowed or denied to networks other than the specified network. After selecting this option, specify the IP address and netmask of the destination network. • **to domain name**–Access is allowed or denied to the specified domains. After selecting this option, specify the domain name in the **Domain Name** text box. • **to master IP**–Access is allowed or denied to the master IP address.
Log	Select this checkbox if you want a log entry to be created when this rule is triggered. Instant supports firewall based logging function. Firewall logs on the W-IAPs are generated as security logs.
Blacklist	Select the **Blacklist** checkbox to blacklist the client when this rule is triggered. The blacklisting lasts for the duration specified as **Auth failure blacklist time** on the Blacklisting tab of the **Security** window. For more information, see Blacklisting Clients on page 171.
Disable scanning	Select **Disable scanning** checkbox to disable ARM scanning when this rule is triggered. The selection of the **Disable scanning** applies only if ARM scanning is enabled, For more information, see Configuring Radio Settings for a W-IAP on page 238.
DSCP tag	Select the **DSCP tag** checkbox to specify a DSCP value to prioritize traffic when this rule is triggered. Specify a value within the range of 0 to 63. To assign a higher priority, specify a higher value.
802.1p priority	Select the **802.1p priority** checkbox to specify an 802.1p priority. Specify a value between 0 and 7. To assign a higher priority, specify a higher value.

3. Click **OK** and then click **Finish**.

In the CLI

To configure access rules:

```
(Instant AP)(config)# wlan access-rule <access-rule-name>
(Instant AP)(Access Rule <Name>)#rule <dest> <mask> <match/invert> {app <app> {permit|deny}
|appcategory <appgrp>}[<option1....option9>]
(Instant AP)(Access Rule <Name>)# end
```

```
(Instant AP)# commit apply
```

Example

```
(Instant AP)(config)# wlan access-rule employee
(Instant AP)(Access Rule "employee")# rule any any match app deny throttle-downstream 256
throttle-up 256
(Instant AP)(Access Rule "employee")# rule any any match appcategory collaboration permit
(Instant AP)(Access Rule "employee")# end
(Instant AP)# commit apply
```

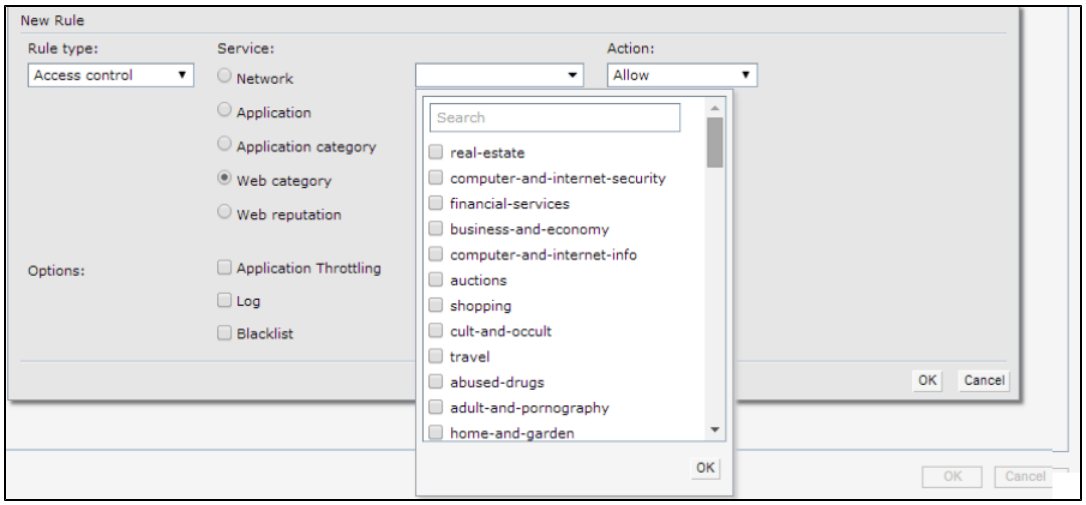
Configuring Web Policy Enforcement

You can configure Web Policy Enforcement on a W-IAP to block certain categories of websites based on your organization specifications by defining ACL rules either through the Instant UI or CLI.

In the Instant UI

1. Navigate to **Security >Roles**.
2. Select any WLAN SSID or wired profile role, and click **New** in the Access Rules section. The **New Rule window** appears.
3. Select the rule type as **Access Control**.
4. To set an access policy based on the web category:
   a. Under **Services**, select **Web category** and expand the **Web categories** drop-down.

Figure 84



   b. Select the categories to which you want to deny or allow access. You can also search for a web category and select the required option.
   c. From the **Action** drop-down, select **Allow** or **Deny** as required.
   d. Click **OK**.
5. To filter access based on the security ratings of the website:
   a. Select **Web reputation** under **Services**.
   b. Move the slider to the required security rating level. Move the slider to select a specific web reputation value to deny access to websites with a reputation value lower than or equal to the configured value or to permit access to websites with a reputation value higher than or equal to the configured value. The following options are available:
      - Trustworthy - These are well known sites with strong security practices and may not expose the user to security risks. There is a very low probability that the user will be exposed to malicious links or payloads.

- Low risk - These are benign sites and may not expose the user to security risks. There is a low probability that the user will be exposed to malicious links or payloads.
- Moderate risk - These are generally benign sites, but may pose a security risk. There is some probability that the user will be exposed to malicious links or payloads.
- Suspicious - These are suspicious sites. There is a higher than average probability that the user will be exposed to malicious links or payloads.
- High risk - These are high risk sites. There is a high probability that the user will be exposed to malicious links or payloads.

c. From the **Action** drop-down, select **Allow** or **Deny** as required.

6. To set a bandwidth limit based on web category or web reputation score, select **Application Throttling** checkbox and specify the downstream and upstream rates in Kbps. For example, you can set a higher bandwidth for trusted sites and a low bandwidth rate for high risk sites.
7. If required, select the following checkboxes:
   - **Log**–Select this checkbox if you want a log entry to be created when this rule is triggered. Instant supports firewall based logging function. Firewall logs on the W-IAPs are generated as security logs.
   - **Blacklist**–Select the **Blacklist** checkbox to blacklist the client when this rule is triggered. The blacklisting lasts for the duration specified as **Auth failure blacklist time** on the Blacklisting tab of the **Security** window. For more information, see Blacklisting Clients on page 171.
   - **Disable scanning**–Select **Disable scanning** checkbox to disable ARM scanning when this rule is triggered. The selection of the **Disable scanning** applies only if ARM scanning is enabled, For more information, see Configuring Radio Settings for a W-IAP on page 238.
   - **DSCP tag**–Select the **DSCP tag** checkbox to specify a DSCP value to prioritize traffic when this rule is triggered. Specify a value within the range of 0 to 63. To assign a higher priority, specify a higher value.
   - **802.1p priority**–Select the **802.1p priority** checkbox to specify an 802.1p priority. Specify a value between 0 and 7. To assign a higher priority, specify a higher value.
8. Click **OK** to save the rules.
9. Click **OK** in **Roles** tab to save the changes to the role for which you defined ACL rules.

In the CLI

To control access based on web categories and security ratings:

```
(Instant AP)(config)# wlan access-rule <access_rule>
(Instant AP) (Access Rule "<access-rule>")# rule <dest> <mask> <match> webcategory <webgrp>
{permit| deny}[<option1....option9>]
(Instant AP) (Access Rule "<access-rule>")# rule <dest> <mask> <match> webreputation <webrep>
{permit|deny}[<option1....option9>]
(Instant AP) (Access Rule "<access-rule>")# end
(Instant AP)# commit apply
```

Example

```
(Instant AP)(config)# wlan access-rule URLFilter
(Instant AP) (Access Rule "URLFilter")# rule any any match webcategory gambling deny
(Instant AP) (Access Rule "URLFilter")# rule any any match webcategory training-and-tools
permit
(Instant AP) (Access Rule "URLFilter")# rule any any match webreputation suspicious-sites deny
(Instant AP) (Access Rule "URLFilter")# end
(Instant AP)# commit apply
```

This chapter the steps required to configure voice and video services on a W-IAP for Voice over IP (VoIP) devices, including Session Initiation Protocol (SIP), Spectralink Voice Priority (SVP), H323, SCCP, Vocera, and Alcatel NOE phones, clients running Microsoft OCS, and Apple devices running the Facetime application.

This section includes the following topics:

- Wi-Fi Multimedia Traffic Management on page 251
- QoS for Microsoft Office OCS and Apple Facetime on page 253

Wi-Fi Multimedia Traffic Management

Wi-Fi Multimedia (WMM), is a Wi-Fi Alliance specification based on the IEEE 802.11e wireless Quality of Service (QoS) standard. WMM works with 802.11a, b, g, and n physical layer standards.

WMM supports the following access categories (ACs):

- Voice
- Video
- Best effort
- Background

The following table shows the mapping of the WMM access categories to 802.1p priority values. The 802.1p priority value is contained in a two-byte QoS control field in the WMM data frame.

Table 50: *WMM AC to 802.1p Priority Mapping*

802.1p Priority	WMM Access Category
1	Background
2	
0	Best effort
3	
4	Video
5	
6	Voice
7	

In a non-WMM or hybrid environment, where some clients are not WMM-capable, you can configure an SSID with higher values for best effort and voice ACs, to allocate a higher bandwidth to clients transmitting best effort and voice traffic.

Configuring WMM for Wireless Clients

You can configure WMM for wireless clients by using the UI or CLI.

In the Instant UI

1. Navigate to the WLAN wizard (click **Network**>**New** or **Network**> Select the WLAN SSID>**edit**).
2. Click **Show advanced options** under **WLAN Settings**.
3. Specify a percentage value for the following WMM access categories in the corresponding **Share** field. You can allocate a higher bandwidth for voice and video traffic than other types of traffic based on the network profile.
   - **Background WMM** – Allocates bandwidth for background traffic such as file downloads or print jobs.
   - **Best effort WMM** –Allocates bandwidth or best effort traffic such as traffic from legacy devices or traffic from applications or devices that do not support QoS.
   - **Video WMM** – Allocates bandwidth for video traffic generated from video streaming.
   - **Voice WMM** – Allocates bandwidth for voice traffic generated from the incoming and outgoing voice communication.

   In a non-WMM or hybrid environment, where some clients are not WMM-capable, you can allocate higher values for **Best effort WMM** and **Voice WMM** to allocate a higher bandwidth to clients transmitting best effort and voice traffic.
4. Click **Next** and complete the configuration as required.

In the CLI

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# wmm-background-share <share>
(Instant AP)(SSID Profile <name>)# wmm-best-effort-share <share>
(Instant AP)(SSID Profile <name>)# wmm-video-share <share>
(Instant AP)(SSID Profile <name>)# wmm-voice-share <share>
(Instant AP)(SSID Profile <name>)# end
(Instant AP)# commit apply
```

Configuring WMM-DSCP Mapping

The IEEE 802.11e standard defines the mapping between WMM ACs and Differentiated Services Codepoint (DSCP) tags.You can customize the mapping values between WMM ACs and DSCP tags to prioritize various traffic types and apply these changes to a WMM-enabled SSID profile.

DSCP classifies packets based on network policies and rules. The following table shows the default WMM AC to DSCP mappings and the recommended WMM AC to DSCP mappings.

Table 51: *WMM-DSCP Mapping*

DSCP Value	WMM Access Category
8	Background
16	
0	Best effort
24	
32	Video
40	
48	Voice
56	

By customizing WMM AC mappings, all packets received are matched against the entries in the mapping table and prioritized accordingly. The mapping table contains information for upstream (client to W-IAP) and downstream (W-IAP to client) traffic.

You can configure different WMM to DSCP mapping values for each WMM AC when configuring an SSID profile either in the Instant UI or CLI.

In the Instant UI

1. Navigate to the WLAN wizard (click **Network**>**New** or **Network**> Select the WLAN SSID>**edit**).
2. Click **Show advanced options** under **WLAN Settings**.
3. Specify the appropriate DSCP mapping value within a range of 0-63 for the following access categories in the **DSCP mapping** field:
   - **Background WMM** – DSCP mapping for the background traffic.
   - **Best effort WMM** – DSCP mapping for the best-effort traffic.
   - **Video WMM** – DSCP mapping for the video traffic.
   - **Voice WMM** – DSCP mapping for the voice traffic.
4. Click **Next** and complete the configuration as required.

In the CLI

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# wmm-background-dscp <dscp>
(Instant AP)(SSID Profile <name>)# wmm-best-effort-dscp <dscp>
(Instant AP)(SSID Profile <name>)# wmm-video-dscp <dscp>
(Instant AP)(SSID Profile <name>)# wmm-voice-dscp <dscp>
(Instant AP)(SSID Profile <name>)# end
(Instant AP)# commit apply
```

You can configure up to 8 DSCP mappings values within the range of 0-63. You can also configure a combination of multiple values separated by a comma, for example, **wmm-voice-dscp 46,44,42,41**.

QoS for Microsoft Office OCS and Apple Facetime

Voice and video devices use a signaling protocol to establish, control, and terminate voice and video calls. These control or signaling sessions are usually permitted using pre-defined ACLs. If the control signaling packets are encrypted, the W-IAP cannot determine the dynamic ports are used for voice or video traffic. In these cases, the W-IAP has to use an ACL with the classify-media option enabled to identify the voice or video flow based on a deep packet inspection and analysis of the actual traffic. Instant identifies and prioritizes voice and video traffic from applications such as Microsoft Office Communications Server (OCS) and Apple Facetime.

Microsoft OCS

Microsoft Office Communications Server (OCS) uses Session Initiation Protocol (SIP) over TLS to establish, control, and terminate voice and video calls.

Apple Facetime

When an Apple device starts a Facetime video call, it initiates a TCP session to the Apple Facetime server over port 5223, then sends SIP signaling messages over a non-default port. When media traffic starts flowing, audio and video data are sent through that same port using RTP. (The audio and video packets are interleaved in the air, though individual the sessions can be uniquely identified using their payload type and sequence numbers.) The RTP header and payload also get encapsulated under the TURN ChannelData Messages. The Facetime call is terminated with a SIP BYE message that can be sent by either party.

The following table lists the ports used by Apple Facetime. Facetime users need to be assigned a role where traffic is allowed on these ports.

Table 52: *Ports Used by the Apple Facetime Application*

Port	Packet Type
53	TCP/UDP
443	TCP
3478-3497	UDP
5223	TCP
16384-16387	UDP
16393-16402	UDP

This chapter provides information on how to configure following services on a W-IAP:

- AirGroup
- Real Time Location Server (RTLS)
- Analytics and Location Engine (ALE)
- OpenDNS
- Communications Assistance for Law Enforcement Act (CALEA)
- Palo Alto Network Firewall
- XML-API Server

AirGroup Configuration

AirGroup provides a unique enterprise-class capability that leverages zero configuration networking to enable AirGroup services from mobile devices in an efficient manner. Zero configuration networking enables service discovery, address assignment, and name resolution for desktop computers, mobile devices, and network services. It is designed for flat, single-subnet IP networks such as wireless networking at home. The users can register their personal devices and define a group of users who can to share the registered devices. Administrators can register and manage an organization's shared devices such as printers and grant global access to each device, or restrict access according to the username, role, or user location.

In large universities and enterprise networks, it is common for devices to connect to the network across VLANs. As a result, user devices on a specific VLAN cannot discover service that resides on another VLAN. As the addresses used by the protocol are link-scope multicast addresses, each query or advertisement can only be forwarded on its respective VLAN, but not across different VLANs. Broadcast and multicast traffic are usually filtered out from a wireless LAN network to preserve the airtime and battery life. This inhibits the performance of AirGroup services that rely on multicast traffic. Dell addresses this challenge with AirGroup technology.

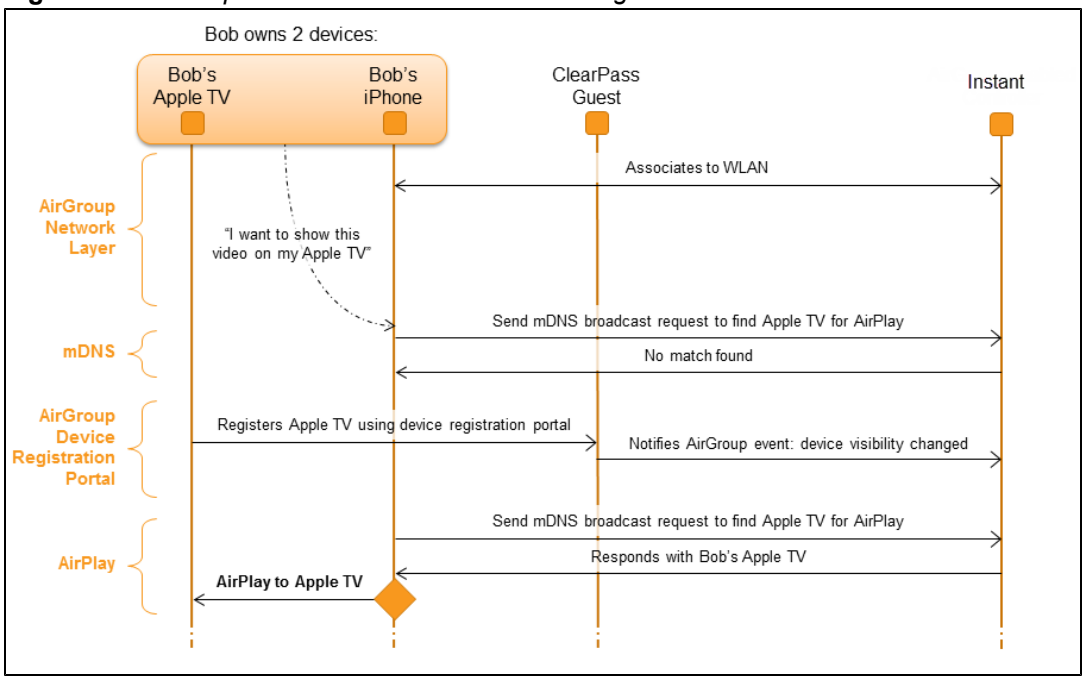
The distributed AirGroup architecture allows each W-IAP to handle mDNS and DLNA queries and responses individually instead of overloading a Virtual Controller with these tasks. This results in a scalable AirGroup solution.

The AirGroup solution supports both wired and wireless devices. An AirGroup device can be registered by an administrator or a guest user.

1. The AirGroup administrator gives an end user the AirGroup operator role, which authorizes the user to register the client devices on the CPPM platform.
2. W-IAPs maintain information for all AirGroup services. W-IAP queries CPPM to map each device’s access privileges to the available services and responds to the query made by a device based on contextual data such as user role, username, and location.

The following figure illustrates how AirGroup enables personal sharing of Apple devices:

Figure 85 *AirGroup Enables Personal Device Sharing*


Bob owns 2 devices:
Bob's Apple TV
Bob's iPhone
ClearPass Guest
Instant
Associates to WLAN
AirGroup Network Layer
"I want to show this video on my Apple TV"
Send mDNS broadcast request to find Apple TV for AirPlay
mDNS
No match found
AirGroup Device Registration Portal
Registers Apple TV using device registration portal
Notifies AirGroup event: device visibility changed
Send mDNS broadcast request to find Apple TV for AirPlay
AirPlay
Responds with Bob's Apple TV
AirPlay to Apple TV

NOTE

AirGroup is not supported on a 3G and PPPoE uplinks.

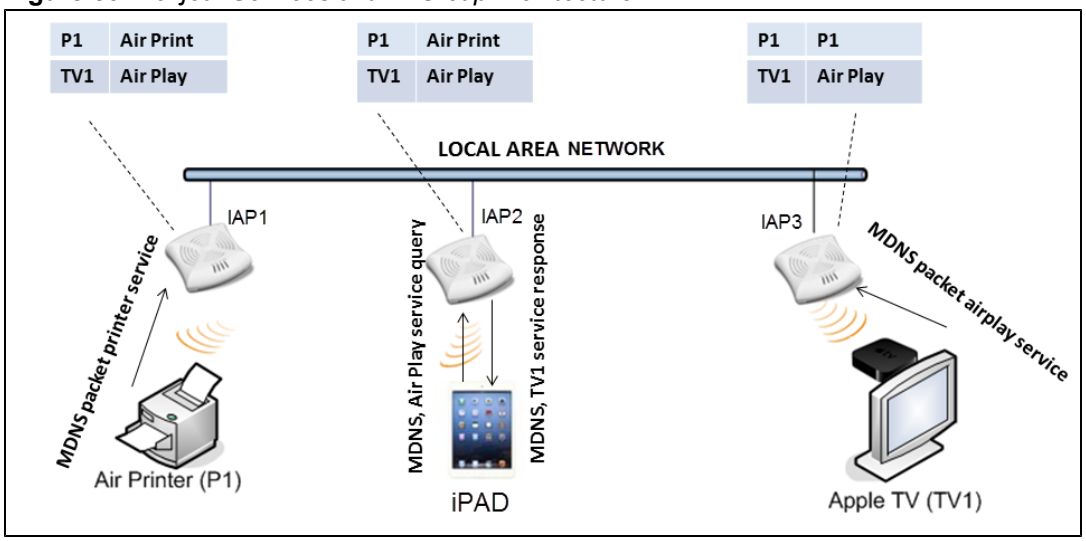
Multicast DNS and Bonjour® Services

Bonjour is the trade name for the zero configuration implementation introduced by Apple. It is supported by most of the Apple product lines, including the Mac OS X operating system, iPhone, iPod Touch, iPad, Apple TV, and AirPort Express. Apple AirPlay and AirPrint services are based on the Bonjour protocol and are essential services in campus Wi-Fi networks.

Bonjour can be installed on computers running Microsoft Windows® and is supported by the new network-capable printers. Bonjour is also included with popular software programs such as Apple iTunes, Safari, and iPhoto. Bonjour uses multicast DNS (mDNS) to locate devices and the services offered by these devices.

As shown in the following figure, the W-IAP1 discovers AirPrint (P1) and W-IAP3 discovers Apple TV (TV1). W-IAP1 advertises information about its connected P1 device to the other W-IAPs that isW-IAP2 and W-IAP3. Similarly, W-IAP3 advertises TV1 device to W-IAP1 and W-IAP2. This type of distributed architecture allows any W-IAP to respond to its connected devices locally. In this example, the iPad connected to W-IAP2 obtains direct response from the same W-IAP about the other Bonjour-enabled services in the network.

Figure 86 *Bonjour Services and AirGroup Architecture*



For a list of supported Bonjour services, see AirGroup Services on page 259.

DLNA UPnP Support

In addition to the mDNS protocol, W-IAPs now support Universal Plug and Play (UPnP) and DLNA (Digital Living Network Alliance) enabled devices. DLNA is a network standard derived from UPnP, which enables devices to discover the services available in a network. DLNA also provides the ability to share data between the Windows or Android based multimedia devices. All the features and policies applicable to mDNS are extended to DLNA to ensure full interoperability between compliant devices.

In a UPnP based scenario, the following types of devices are available in a network:

- Controlled devices (servers)
- Control points (clients)

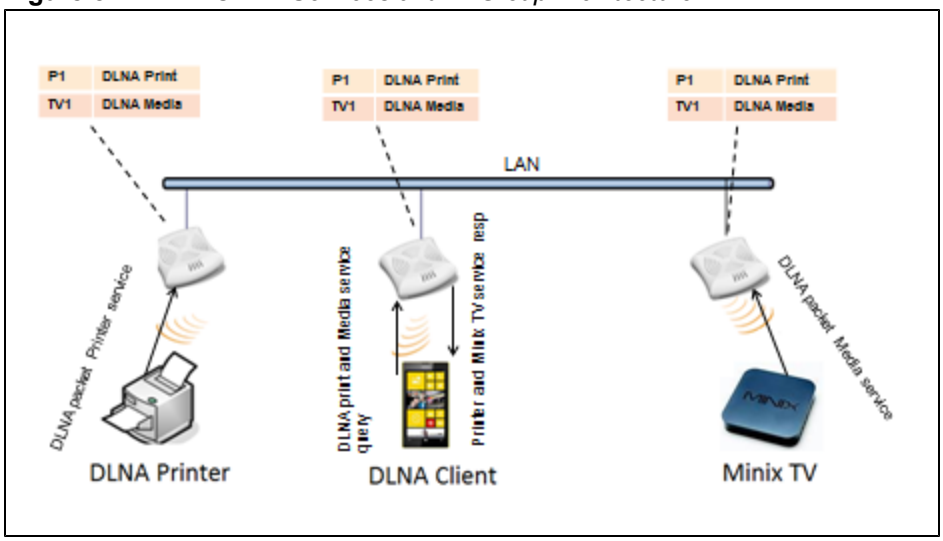
When a controlled device joins a network and acquires IP address, it multicasts a number of discovery messages advertising itself, its embedded devices and services. On the other hand, when a control point joins a network, it may multicast a search discovery message searching for interesting devices and services. The devices listening on the multicast address respond if they match the search criteria in the search message.

In a single AP network, the W-IAP maintains a cache table containing the list of discovered services in the network. The W-IAP also enforces native policies such as disallowing roles and VLANs and the policies defined on CPPM to determine the devices or services that are allowed and can be discovered in the network. Whenever a search request comes, the AP looks up its cache table and filters based on configured policies and then builds a search response and unicasts it to the requesting device.

In a W-IAP cluster, the W-IAPs maintain a list of associated UPnP devices and allow the discovery of the associated devices.

The following figure illustrates DLNA UPnP Services and AirGroup Architecture.

Figure 87 *DLNA UPnP Services and AirGroup Architecture*



For a list of supported DLNA services, see AirGroup Services on page 259.

AirGroup Features

AirGroup supports the following features:

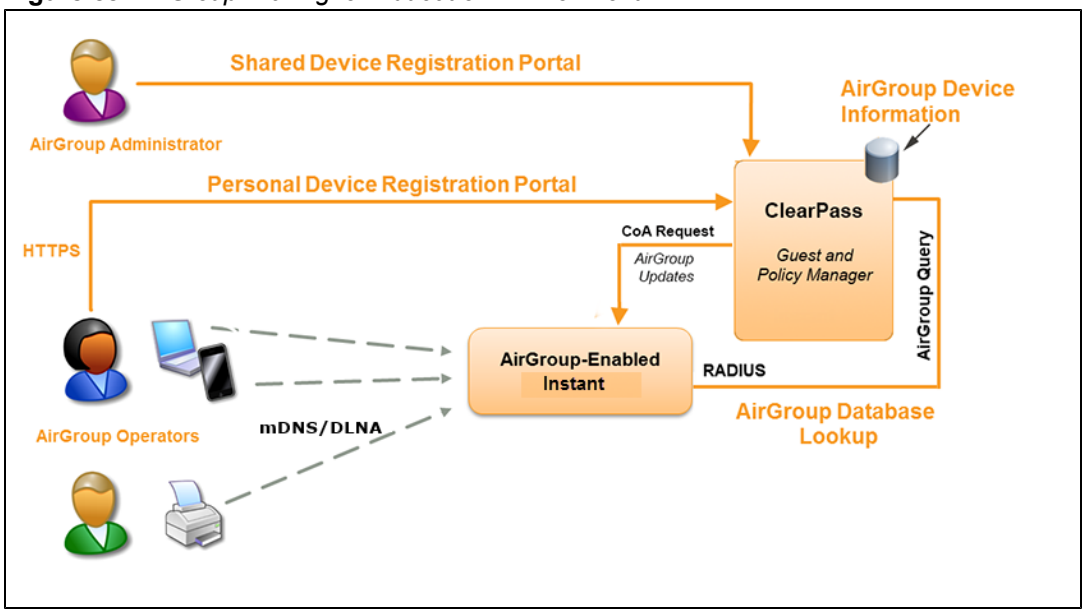
- Sends unicast responses to mDNS or DLNA queries and reduces the traffic footprint.
- Ensures cross-VLAN visibility and availability of AirGroup devices and services.
- Allows or blocks AirGroup services for all users.
- Allows or blocks AirGroup services based on user roles.
- Allows or blocks AirGroup services based on VLANs.
- Matches devices to their closest services such as printers

AirGroup also enables context awareness for services across the network:

- AirGroup is aware of personal and shared devices. For example, an Apple TV in a dorm room can be associated with the student who owns it or an Apple TV in a meeting room or a printer in a supply room that is available to certain users, such as the marketing department.
- AirGroup is aware of the location of services when CPPM support is enabled. For example, depending on proximity, a user would be presented with the closest printer instead of all the printers in the building.
- When configured, AirGroup enables a client to perform a location-based discovery. For example, when a client roams from one Instant cluster to another, it can discover devices available in the new cluster to which the client is currently connected.

The following figure shows an example of a higher-education environment with shared, local, and personal services available to mobile devices.

Figure 88 *AirGroup in a Higher-Education Environment*



NOTE

When AirGroup discovers a new device, it interacts with CPPM to obtain the shared attributes such as shared location and role. However, the current versions of W-IAPs do not support the enforcement of shared location policy.

AirGroup Services

AirGroup supports zero configuration services. The services are pre-configured and are available as part of the factory default configuration. The administrator can also enable or disable any or all services by using the Instant UI or CLI.

The following services are available for W-IAP clients:

- AirPlay™– Apple® AirPlay allows wireless streaming of music, video, and slideshows from your iOS device to Apple TV® and other devices that support the AirPlay feature.
- AirPrint™– Apple AirPrint allows you to print from an iPad®, iPhone®, or iPod® Touch directly to any AirPrint compatible printers.
- iTunes–The iTunes service is used by iTunes Wi-Fi sync and iTunes home-sharing applications across all Apple devices.
- RemoteMgmt–The RemoteMgmt service allows remote login, remote management, and FTP utilities on Apple devices.
- Sharing– The Sharing service allows applications such as disk sharing and file sharing among Apple devices.
- Chat– The iChat® (Instant Messenger) application on Apple devices uses this service.
- ChromeCast–ChromeCast service allows you to use a ChromeCast device to play audio or video content on a high definition television by streaming content through Wi-Fi from the Internet or local network.
- DLNA Media–Applications such as Windows Media Player use this service to browse and play media content on a remote device.
- DLNA Print–This service is used by printers that support DLNA.

NOTE

In the Instant 6.4.0.2-4.1 release, it is recommended to have a maximum of upto 80 AirGroup servers in the network

For more information on configuring AirGroup services, see Configuring AirGroup and AirGroup Services on a W-IAP on page 261.

AirGroup Components

AirGroup leverages key elements of the Dell solution portfolio including operating system software for Instant, CPPM, and the VLAN-based or role-based filtering options offered by the AirGroup services. The components that make up the AirGroup solution include the Instant, CPPM, and ClearPass Guest. The version requirements are described in the following table:

Table 53: *Instant, CPPM, and ClearPass Guest Requirements*

Component	Minimum Version for mDNS Services	Minimum Version for DLNA Services
Instant	6.2.0.0-3.2.0.0	6.4.0.2-4.1
ClearPass Guest software	5.2	6.2
ClearPass Guest Services plugin	6.2.0	6.3.0

Starting from ClearPass version 6.0, the ClearPass Guest and the AirGroup Services plug-in are integrated into a single platform.

AirGroup maintains seamless connectivity between clients and services across VLANs and SSIDs. The following table summarizes the filtering options supported by Instant:

Table 54: *AirGroup Filtering Options*

Features	Instant Deployment Models	
	Integrated	**Integrated with CPPM**
Allow mDNS and DLNA traffic to propagate across subnets/VLANs	Yes	Yes
Limit mDNS and DLNA traffic on the network	Yes	Yes
VLAN based AirGroup service policy enforcement	Yes	Yes
User-role based AirGroup service policy enforcement	Yes	Yes
Portal to self register personal leaves	No	Yes
Device owner based policy enforcement	No	Yes
Location based policy enforcement	No	Yes
Shared user list based policy enforcement	No	Yes
Shared role list based policy enforcement	No	Yes

CPPM and ClearPass Guest Features

CPPM and ClearPass Guest support the following features:

- Registration portal for WLAN users to register their personal devices.
- Registration portal for WLAN administrators to register shared devices.
- Operator-defined *personal* AirGroup to specify a list of other users who can share devices with the operator.
- Administrator defined username, user role, and location attributes for shared devices.

Configuring AirGroup and AirGroup Services on a W-IAP

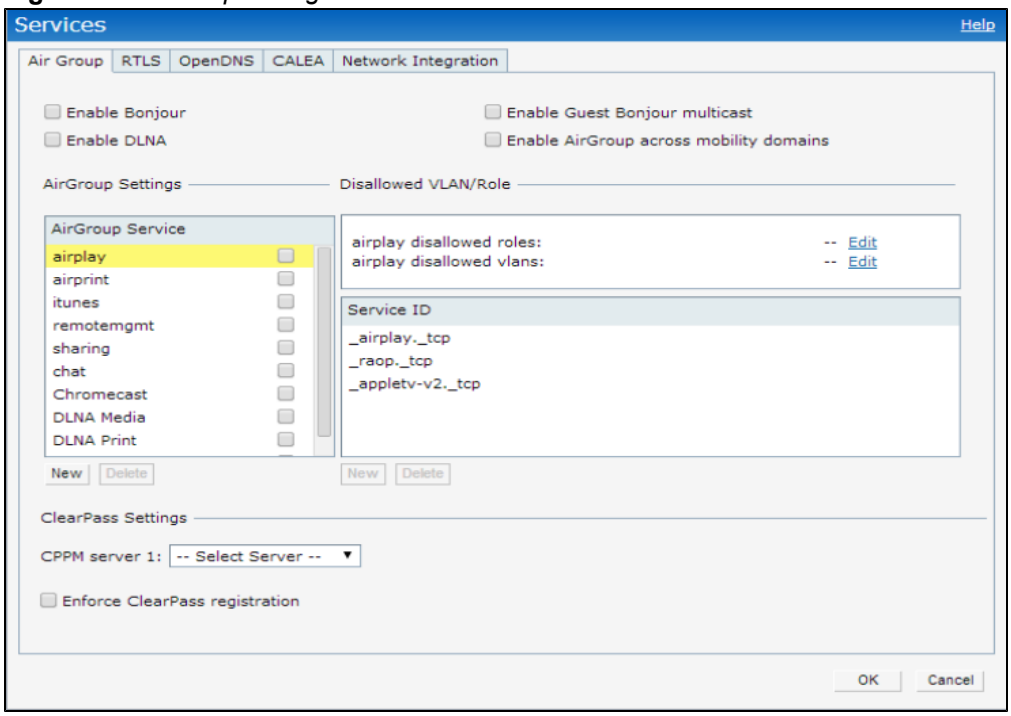
You can configure AirGroup services, using the Instant UI or CLI.

In the Instant UI

To enable AirGroup and its services:

1. Click the **More** > **Services** link at the top right corner of the Instant main window.
2. Click the **Air Group** tab. The **Air Group** tab details are displayed.

Figure 89 *AirGroup Configuration*



3. To enable support for Bonjour services, select the **Enable Bonjour** checkbox and select the AirGroup services related to Bonjour as required.
4. To enable DLNA support, select the **Enable DLNA** checkbox and select the DLNA services.
5. To allow the users to use Bonjour services enabled in a guest VLAN, select **Enable Guest Bonjour multicast**. When this checkbox is enabled, the Bonjour devices are visible only in the guest VLAN and AirGroup will not discover or enforce policies in guest VLAN.
6. Select the **Enable Air Group across mobility domains** checkbox to enable inter-cluster mobility. When enabled, the W-IAP shares the mDNS database information with the other clusters. The DNS records in the Virtual Controller can be shared with the all the Virtual Controllers configured for L3 Mobility.

   By default, this feature is disabled. To define clusters, go to **System**> **L3 Mobility** tab.
7. Ensure that the required AirGroup services are selected. To add any service, click **New** and add. To allow all services, select **allowall**. If a custom service is added, you can add a corresponding service ID by clicking **New** under **Service ID**.

If the W-IAP is upgraded to current release and if Bonjour is enabled, ensure that the corresponding Bonjour services are selected.

Instant supports the use of upto 6 custom services.

8. Based on the services configured, you can block any user roles from accessing an AirGroup service and restrict the AirGroup servers connected to a specific set of VLANs from being discovered . The user roles and VLANs

marked as disallowed are prevented from accessing the corresponding AirGroup service. You can create a list of disallowed user roles and VLANs for all AirGroup services configured on the W-IAP. For example, If the AirPlay service is selected, the **edit** links for the **airplay disallowed roles** and **airplay disallowed vlans** are displayed. Similarly, if sharing service is selected, the **edit** links for the **sharing disallowed roles** and **sharing disallowed vlans** are displayed.

- To select block user roles from accessing an AirGroup service, click the corresponding **edit** link and select the user roles for which you want to restrict access. By default, an AirGroup service is accessible by all user roles configured in your W-IAP cluster.
- To select VLANs from allowing access to an AirGroup service, click the corresponding **edit** link and select the VLANs to exclude. By default, the AirGroup services are accessible by users or devices in all VLANs configured in your W-IAP cluster.

9. **ClearPass Settings**– Use this section to configure the CPPM server, CoA server, and enforce ClearPass registering.
   - **CPPM server 1**– Indicates the ClearPass Policy Manager server information for AirGroup policy.
   - **Enforce ClearPass registering**– When enabled, only devices registered with CPPM will be discovered by Bonjour devices, based on the CPPM policy.

In the CLI

To configure AirGroup:

```
(Instant AP)(config)# airgroup
(Instant AP)(airgroup)# enable [dlna-only| mdns-only]
(Instant AP)(airgroup)# cppm enforce-registration
(Instant AP)(airgroup)# cppm-server <server>
(Instant AP)(airgroup)# cppm-query-interval <interval>
(Instant AP)(airgroup)# disallow-vlan <vlan-ID>
(Instant AP)(airgroup)# enable-guest-multicast
(Instant AP)(airgroup)# multi-swarm
(Instant AP)(airgroup)# end
(Instant AP)# commit apply
```

To enable DLNA support:

```
(Instant AP)(config)# airgroup
(Instant AP)(airgroup)# enable dlna-only
(Instant AP)(airgroup)# end
(Instant AP)# commit apply
```

To enable support for Bonjour services:

```
(Instant AP)(config)# airgroup
(Instant AP)(config)# enable mdns-only
(Instant AP)(airgroup)# end
(Instant AP)# commit apply
```

To configure AirGroup Service

```
(Instant AP)(config)# airgroupservice <airgroup-service>
(Instant AP)(airgroup-service)# id <airgroupservice-ID>
(Instant AP)(airgroup-service)# description <text>
(Instant AP)(airgroup-service)# disallow-role <role>
(Instant AP)(airgroup-service)# disallow-vlan <vlan-ID>
(Instant AP)(airgroup-service)# end
(Instant AP)# commit apply
```

To verify the AirGroup configuration status:

```
(Instant AP)# show airgroup status
```

Configuring AirGroup and CPPM interface in Instant

Configure the Instant and CPPM interface to allow an AirGroup W-IAP and CPPM to exchange information regarding device sharing, and location. The configuration options define the RADIUS server that is used by the AirGroup RADIUS client.

The AirGroup configuration with CPPM involves the following steps:

1. Create a RADIUS service
2. Assign a Server to AirGroup
3. Configure CPPM to Enforce Registration

Creating a RADIUS Server

You can configure an external RADIUS Security window. For more information on the configuring CPPM server, see Configuring an External Server for Authentication on page 157. You can also create a RADIUS server in the **Air Group** window. Navigate to **Services > AirGroup > Clear Pass Settings > CPPM server 1 >** and select **New** from the drop-down list.

Assign a Server to AirGroup

To associate the CPPM server with AirGroup, select the CPPM server from the **CPPM Server 1** drop-down list.

If two CPPM servers are configured, the CPPM server 1 acts as a primary server and the CPPM server 2 acts as a backup server.

After the configuration is complete, this particular server will be displayed in the CoA server option. To view this server go to **Services> AirGroup >ClearPass Settings > CoA server**.

Configure CPPM to Enforce Registration

When CPPM registration is enforced, the devices registered with CPPM will be discovered by Bonjour devices, based on the CPPM policy.

Change of Authorization (CoA)

When a RADIUS server is configured with Change of Authorization (CoA) with the CPPM server, the guest users are allowed to register their devices. For more information on configuring RADIUS server with CoA , see Configuring an External Server for Authentication on page 157.

You can also create a **CoA only server** in the **Services > AirGroup > Clear Pass Settings > CoA server** window.

Configuring a W-IAP for RTLS Support

Instant supports the real-time tracking of devices when integrated with the W-AirWave Management Platform, or a third-party Real Time Location Server such as Aeroscout Real Time Location Server. With the help of the RTLS, the devices can be monitored in real-time or through history.

You can configure RTLS using the Instant UI or CLI.

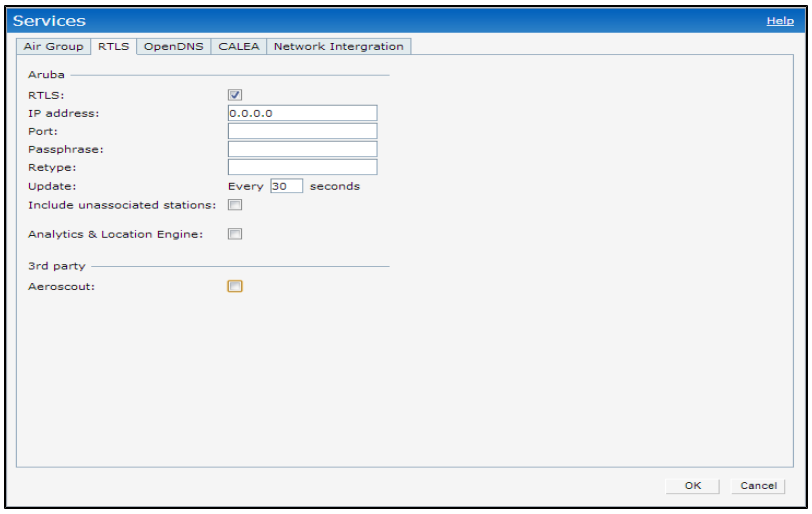
In the Instant UI

To configure Aruba RTLS:

1. Click the **More** > **Services** link at the top right corner of the Instant main window. The **Services** window is displayed.

2. Click the **RTLS** tab. The following figure shows the contents of the **RTLS** tab.
3. Under **Aruba**, select the **RTLS** check-box to integrate Instant with the W-AirWave Management Platform or Ekahau Real Time Location Server.

Figure 90 *RTLS Window*



4. Specify the IP address and port to which the location reports must be sent.
5. Specify the shared secret key in the **Passphrase** text box.
6. Specify the frequency at which the Virtual Controller can send updates to the server. You can specify a value within the range of 5-3600 seconds. The default value is 5 seconds.
7. Select the **Include unassociated stations** check-box to send reports on the stations that are not associated to any W-IAP to the RTLS server.
8. Click **OK**.

To configure third-party RTLS such as Aeroscout:

1. Select the **Aeroscout** check-box to send the RFID tag information to an AeroScout RTLS.
2. Specify the IP address and port number of the AeroScout server, to which location reports must be sent.
3. Select the **Include unassociated stations** check-box to send reports on the stations that are not associated to any W-IAP to the Aeroscout RTLS server.
4. Click **OK**.

In the CLI

To configure W-AirWave RTLS:

```
(Instant AP)(config)# airwave-rtls <IP-address> <port> <passphrase> <seconds> include-unassoc-sta
(Instant AP)(config)# end
(Instant AP)# commit apply
```

To configure Aeroscout RTLS

```
(Instant AP)(config)# aeroscout-rtls <IP-address> <port> include-unassoc-sta
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Configuring a W-IAP for Analytics and Location Engine Support

The Analytics and Location Engine (ALE) is designed to gather client information from the network, process it and share it through a standard API. The client information gathered by ALE can be used for analyzing a client's internet behavior for business such as shopping preferences.

ALE includes a location engine that calculates the associated and unassociated device location every 30 seconds by default. For every device on the network, ALE provides the following information through the Northbound API:

- Client user name
- IP address
- MAC address
- Device type
- Application firewall data, showing the destinations and applications used by associated devices.
- Current location
- Historical location

ALE requires the AP placement data to be able to calculate location for the devices in a network.

ALE with Instant

The Instant 6.3.1.1-4.0 release supports Analytics and Location Engine (ALE). The ALE server acts as a primary interface to all third-party applications and the W-IAP sends client information and all status information to the ALE server.

To integrate W-IAP with ALE, the ALE server address must be configured on a W-IAP. If the ALE sever is configured with a host name, the Virtual Controller performs a mutual certificated-based authentication with ALE server, before sending any information.

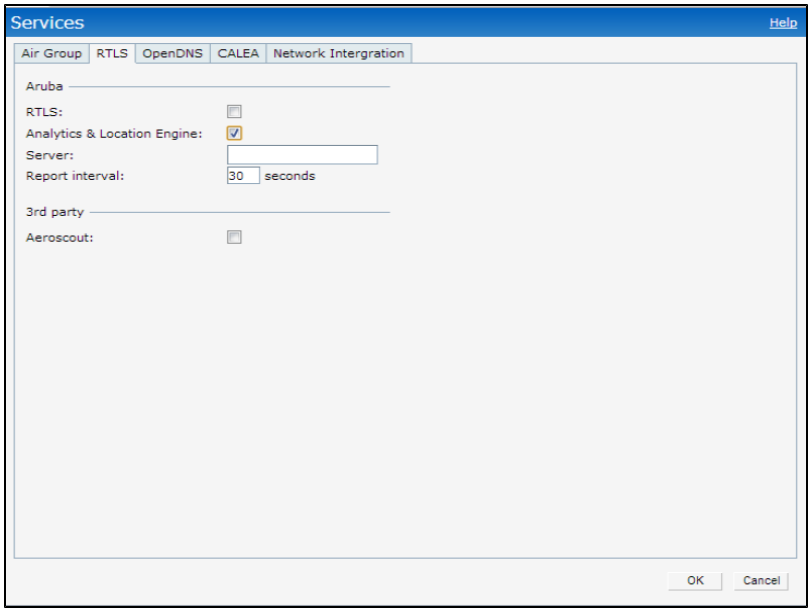
Enabling ALE Support on a W-IAP

You can configure a W-IAP for ALE support using the Instant UI or CLI.

In the Instant UI

1. Click **More > Services**. The **Services** window is displayed.
2. Click the **RTLS** tab. The tab details are displayed.
3. Select the **Analytics & Location Engine** checkbox.

Figure 91 *Services Window —ALE Integration*



4. Specify the ALE server name or IP address.
5. Specify the reporting interval within the range of 6-60 seconds. The W-IAP sends messages to the ALE server at the specified interval. The default interval is 30 seconds.
6. Click **OK**.

In the CLI

To enable W-IAP integration with the ALE server:

```
(Instant AP)(config)# ale-server <server-name| IP-address>
(Instant AP)(config)# ale-report-interval <seconds>
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Verifying ALE Configuration on a W-IAP

To view the configuration details:

```
(Instant AP)# show ale config
```

To verify the configuration status

```
(Instant AP)# show ale status
```

Configuring OpenDNS Credentials

When configured, the OpenDNS credentials are used by Instant to access OpenDNS to provide enterprise-level content filtering. You can configure OpenDNS credentials using the Instant UI or CLI.

In the Instant UI

To configure OpenDNS credentials:

1. Click **More** > **Services** > **OpenDNS**. The **OpenDNS** tab contents are displayed.
2. Enter the **Username** and **Password** to enable access to OpenDNS.
3. Click **OK** to apply the changes.

In the CLI

To configure OpenDNS credentials:

```
(Instant AP)(config)# opendns <username <password>
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Integrating a W-IAP with Palo Alto Networks Firewall

Palo Alto Networks (PAN) next-generation firewall offers contextual security for all users for safe enabling of applications. A simple firewall beyond basic IP address or TCP port numbers only provides a subset of the enhanced security required for enterprises to secure their networks. In the context of businesses using social networking sites, legacy firewalls are not able to differentiate valid authorized users from casual social networking users.

The Palo Alto next-generation firewall is based on user ID, which provides many methods for connecting to sources of identity information and associating them with firewall policy rules. For example, it provides an option to gather user information from Active Directory or LDAP server.

Integration with Instant

The functionality provided by the PAN firewall based on user ID requires the collection of information from the network. W-IAP maintains the network (such as mapping IP address) and user information for its clients in the network and can provide the required information for the user ID feature on PAN firewall. Before sending the user-ID mapping information to the PAN firewall, the W-IAP must retrieve an API key that will be used for authentication for all APIs.

W-IAP and PAN firewall integration can be seamless with the XML-API that available with PAN-OS 5.0 or later.

To integrate a W-IAP with PAN user ID, a global profile is added. This profile can be configured on a W-IAP with PAN firewall information such as IP address, port, user name, password, firewall enabled or disabled status.

The W-IAP sends messages to PAN based on the type of authentication and client status:

- After a client completes the authentication and is assigned an ip address, W-IAP will send the **login** message.
- After a client is disconnected or dissociated from the W-IAP, the W-IAP sends a **logout** message.

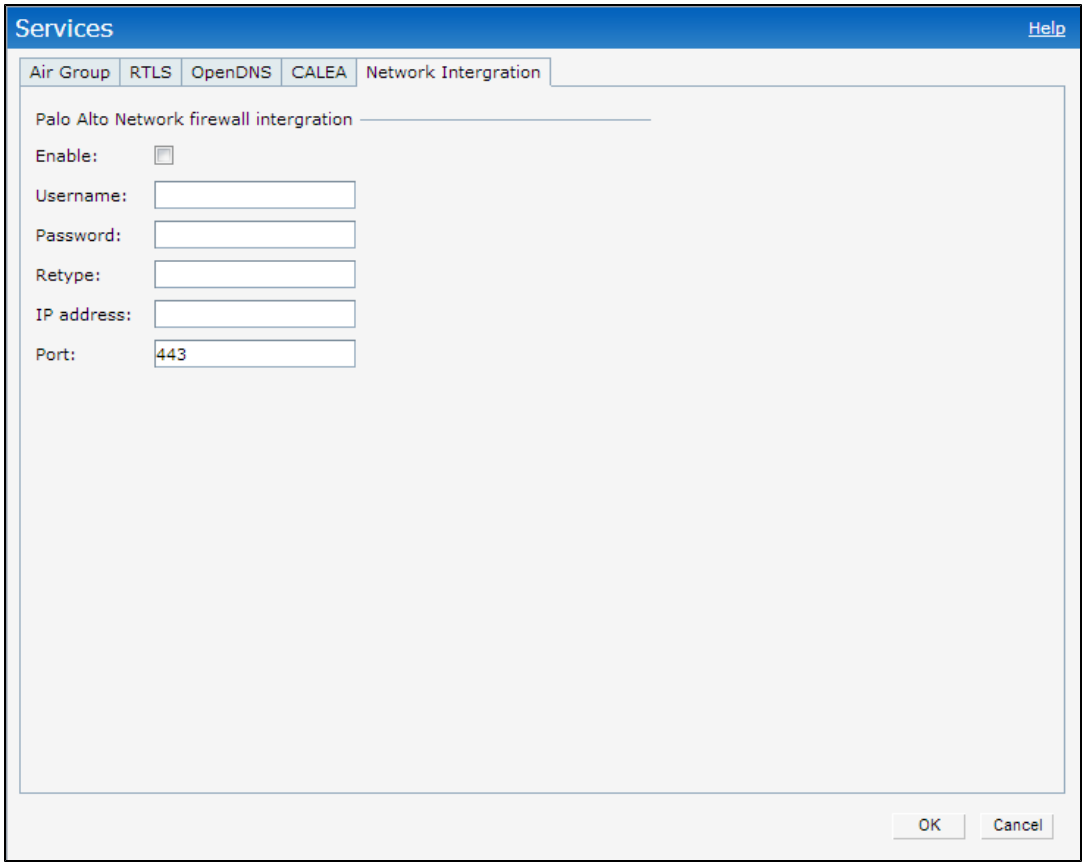
Configuring a W-IAP for PAN integration

You can configure a W-IAP for PAN firewall integration using the Instant UI or CLI.

In the Instant UI

1. Click **More > Services**. The **Services** window is displayed.
2. Click **Network Integration**. The PAN firewall configuration options are displayed.

Figure 92 *Services Window - Network Integration Tab*



3. Select the **Enable** checkbox to enable PAN firewall.
4. Specify the user name and password. Ensure that you provide user credentials of the PAN firewall administrator.
5. Enter the PAN firewall IP address.
6. Enter the port number within the range of 1–65535. The default port is 443.
7. Click **OK**.

In the CLI

To enable PAN firewall integration with the W-IAP:

```
(Instant AP)(config)# firewall-external-enforcement pan
(Instant AP)(firewall-external-enforcement pan)# enable
(Instant AP)(firewall-external-enforcement pan)# ip <ip-address>
(Instant AP)(firewall-external-enforcement pan)# port <port>
(Instant AP)(firewall-external-enforcement pan)# user <name> <password>
(Instant AP)(firewall-external-enforcement pan)# end
(Instant AP)# commit apply
```

Integrating a W-IAP with an XML API interface

The XML API interface provides options to create and execute user management operations seamlessly on behalf of the clients or users.

Integration with Instant

The XML API interface allows users to send specific XML commands to a W-IAP from an external server. These XML commands can be used to customize W-IAP client entries. You can use the XML API interface to add, delete, authenticate, query, or blacklist a user or a client.

The user authentication is supported only for users authenticated by Captive Portal authentication and not for the dot1x-authentication users.

The user add operation performed by the XML API interface is only used to modify the role of an existing user and not to create a new user.

Users can now use HTTP or HTTPS to post commands to W-IAP. The communication process using the XML API Interface is as follows:

- An API command is issued in XML format from the Server to the Virtual Controller.
- The Virtual Controller processes the XML request and identifies where the client is and sends the command to the correct slave W-IAP.
- Once the operation is completed, Virtual Controller sends the XML response to the XML server.
- Users can use the response and take appropriate action that suit their requirements. The response from the controller is returned using predefined formats.

Configuring a W-IAP for XML API integration

You can configure a W-IAP for XML API integration using the Instant UI or CLI.

In the Instant UI

1. Click **More > Services**. The **Services** window is displayed.
2. Click **Network Integration**. The XML API Server configuration options are displayed.

Figure 93 *XML API Server Configuration*

3. Enter the **IP address** of the XML API Server.
4. Enter the **Passphrase** required to authenticate and access the XML API Server.
5. Re-enter the **Passphrase** in the **Retype** box.
6. Click **OK**.

In the CLI

To enable XML API integration with the W-IAP:

```
(Instant AP)(config)# xml-api-server
(Instant AP)(xml-api-server)# ip <ip-address>
(Instant AP)(xml-api-server)# key <shared-key>
(Instant AP)(xml-api-server)# no <delete-command>
(Instant AP)(xml-api-server)# end
(Instant AP)# commit apply
```

CALEA Integration and Lawful Intercept Compliance

Lawful Intercept (LI) allows the Law Enforcement Agencies (LEA) to perform an authorized electronic surveillance. Depending on the country of operation, the service providers (SPs) are required to support LI in their respective networks.

In the United States, SPs are required to ensure LI compliance based on Communications Assistance for Law Enforcement Act (CALEA) specifications.

Instant supports CALEA integration in a hierarchical and flat topology, mesh W-IAP network, the wired and wireless networks.

NOTE

Enable this feature only if lawful interception is authorized by a law enforcement agency.

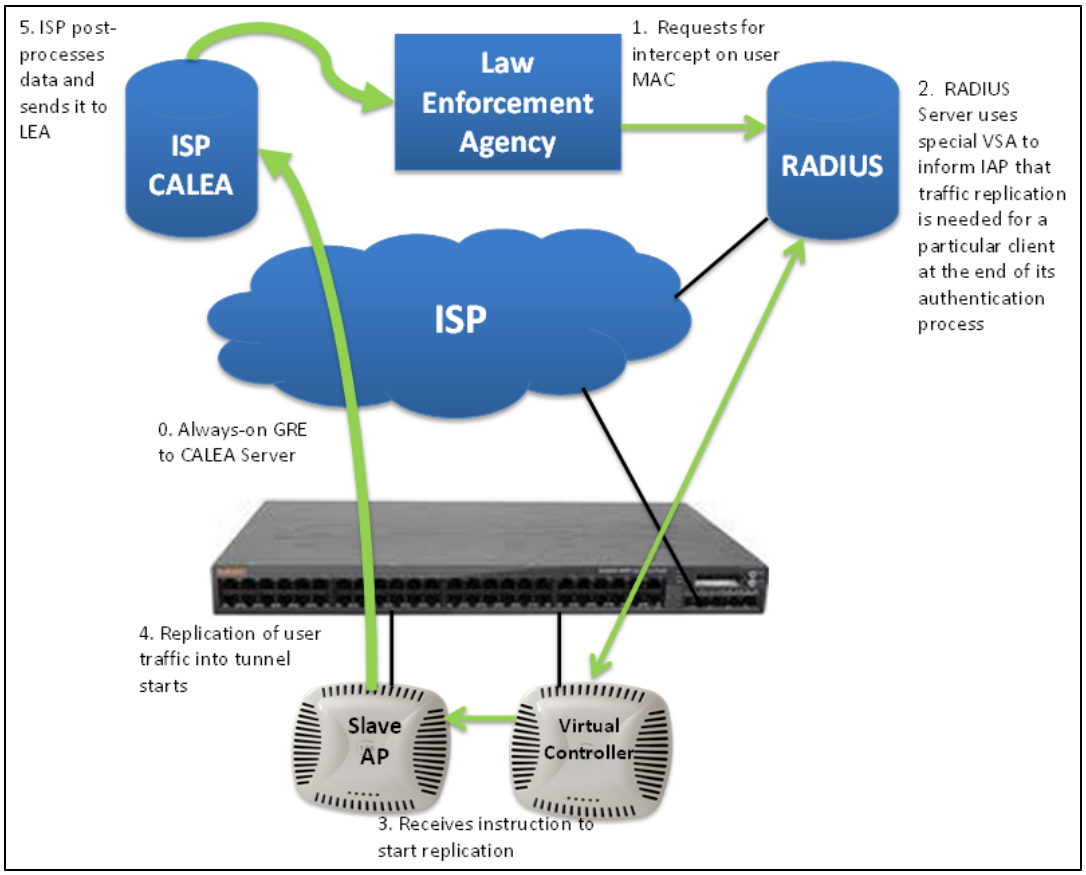
CALEA Server Integration

To support CALEA integration and ensure LI compliance, you can configure the W-IAPs to replicate a specific or selected client traffic and send it to a remote CALEA server.

Traffic Flow from IAP to CALEA Server

You can configure a W-IAP to send GRE encapsulated packets to the CALEA server and replicate client traffic within the GRE tunnel. Each W-IAP sends GRE encapsulated packets only for its associated or connected clients. The following figure illustrates the traffic flow from the W-IAP to the CALEA server.

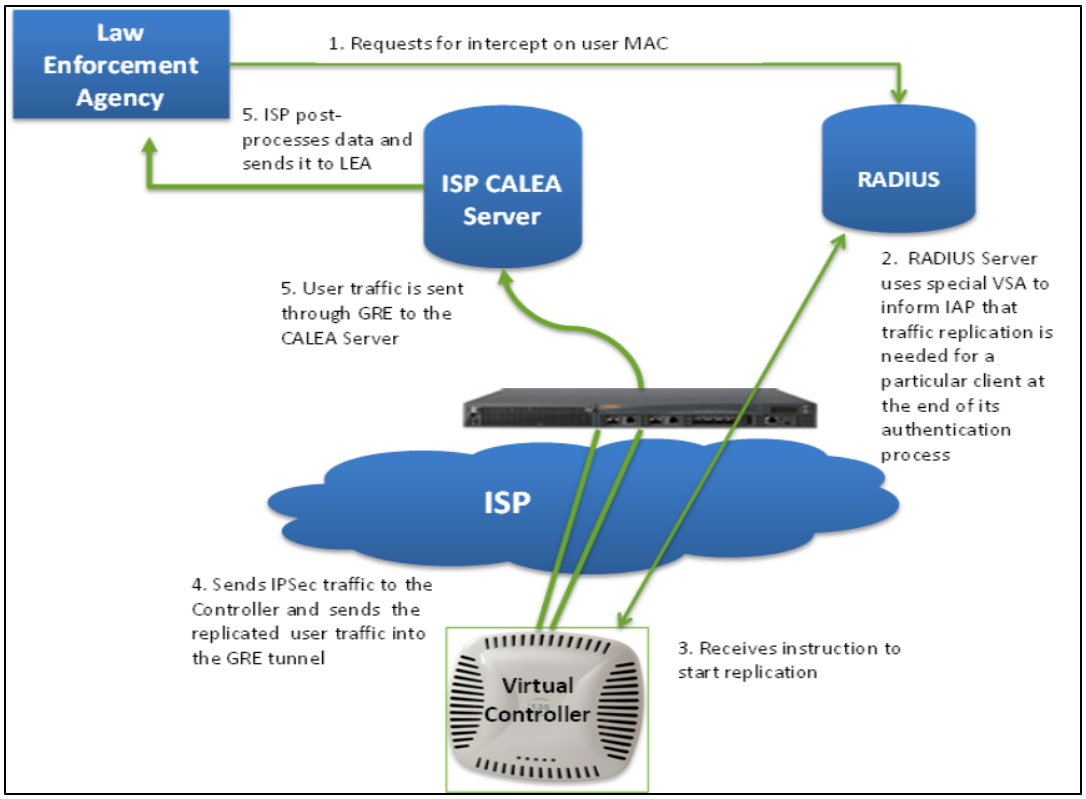
Figure 94 *IAP to CALEA Server*


5. ISP post-processes data and sends it to LEA
ISP CALEA
Law Enforcement Agency
1. Requests for intercept on user MAC
RADIUS
2. RADIUS Server uses special VSA to inform IAP that traffic replication is needed for a particular client at the end of its authentication process
ISP
0. Always-on GRE to CALEA Server
4. Replication of user traffic into tunnel starts
Slave AP
Virtual Controller
3. Receives instruction to start replication

Traffic Flow from IAP to CALEA Server through VPN

You can also deploy the CALEA server with the controller and configure an additional IPSec tunnel for corporate access. When CALEA server is configured with the controller, the client traffic is replicated by the slave W-IAP and client data is encapsulated by GRE on slave, and routed to the master W-IAP. The master IAP sends the IPsec client traffic to the controller. The controller handles the IPSec client traffic while GRE data is routed to the CALEA server. The following figure illustrates the traffic flow from W-IAP to the CALEA server through VPN.

Figure 95 *IAP to CALEA Server through VPN*


Law Enforcement Agency
1. Requests for intercept on user MAC
5. ISP post-processes data and sends it to LEA
ISP CALEA Server
RADIUS
2. RADIUS Server uses special VSA to inform IAP that traffic replication is needed for a particular client at the end of its authentication process
5. User traffic is sent through GRE to the CALEA Server
ISP
4. Sends IPSec traffic to the Controller and sends the replicated user traffic into the GRE tunnel
3. Receives instruction to start replication
Virtual Controller

Ensure that IPSec tunnel is configured if the client data has to be routed to the ISP or CALEA server through VPN. For more information on configuring IPSec, see Configuring an IPSec Tunnel on page 210.

Client Traffic Replication

Client traffic is replicated in the following ways:

- Through RADIUS VSA– In this method, the client traffic is replicated by using the RADIUS VSA to assign clients to a CALEA related user role. To enable role assignment to clients, you need to create a user role and a CALEA access rule, and then assign the CALEA rule to the user role. Whenever a client that is configured to use a CALEA rule connects, a replication role is assigned.
- Through Change of Authorization (CoA)–In this method, a user session can start without replication. When the network administrator triggers a CoA from the RADIUS server, the user session is replicated. The replication is stopped when the user disconnects or by sending a CoA to change the replication role.

As the client information is shared between multiple W-IAPs in a cluster, the replication rules persist when clients roam within the cluster.

Configuring a W-IAP for CALEA Integration

To enable CALEA server integration, perform the following steps:

1. Create a CALEA profile.

2. If a replication role must be assigned through the RADIUS VSA, create an access rule and assign the access rule to a WLAN SSID or wired profile.
3. Verify the configuration.

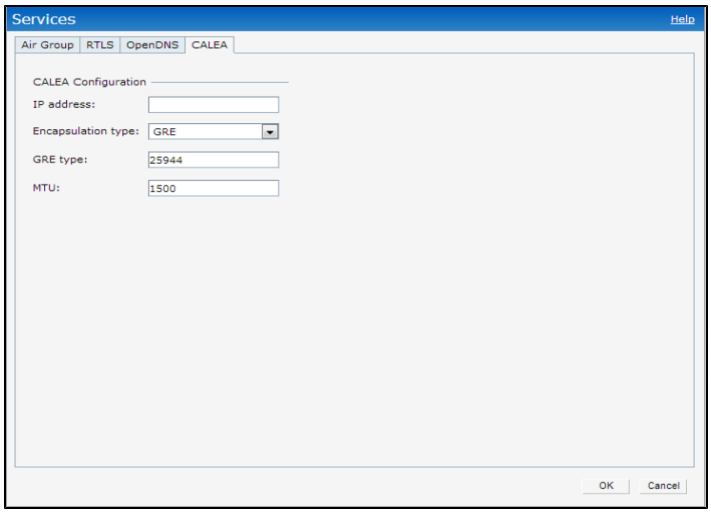
Creating a CALEA Profile

You can create a CALEA profile by using the Instant UI or CLI.

In the Instant UI

To configure a CALEA profile:

1. Click **More** > **Services** at the top right corner of the Instant main window.
2. Click **CALEA**. The **CALEA** tab details are displayed.



3. Specify the following parameters:
   - **IP address**– Specify the IP address of the CALEA server.
   - **Encapsulation type**– Specify the encapsulation type. The current release of Instant supports GRE only.
   - **GRE type**– Specify the GRE type.
   - **MTU**– Specify a size for the maximum transmission unit (MTU) within the range of 68–1500. After GRE encapsulation, if packet length exceeds the configured MTU, IP fragmentation occurs. The default MTU size is 1500.
4. Click **OK**.

In the CLI

```
(Instant AP)(config)# calea
(Instant AP)(calea)# ip <IP-address>
(Instant AP)(calea)# ip mtu <size>
(Instant AP)(calea)# encapsulation-type <gre>
(Instant AP)(calea)# gre-type <type>
(Instant AP)(calea)# end
(Instant AP)# commit apply
```

Creating an Access Rule for CALEA

You can create an access rule for CALEA by using the Instant UI or CLI.

In the Instant UI

To create an access rule:

1. To add the CALEA access rule to an existing profile, select an existing wireless (**Networks** tab > **edit**) or wired (**More** > **Wired** > **Edit**) profile. To add the access rule to a new profile, click **New** under Network tab and create a WLAN profile, or click **More**>**Wired**>**New** and create a wired port profile.
2. In the **Access** tab, select the role for which you want create the access rule.
3. Under **Access Rules**, click **New**. The **New Rule** window is displayed.
4. Select **CALEA**.
5. Click **OK**.
6. Create a role assignment rule if required.
7. Click **Finish**.

In the CLI

To create a CALEA access rule:

```
(Instant AP)(config)# wlan access-rule <name>
(Instant AP)(Access Rule <name>)# calea
(Instant AP)(Access Rule <name>)# end
(Instant AP)# commit apply
```

To assign the CALEA rule to a user role:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name># set-role <attribute>{{equals| not-equals| starts-with| ends-
with|contains}<operator><role>|value-of}
(Instant AP)(SSID Profile <name># end
(Instant AP)(SSID Profile <name># commit apply
```

To associate the access rule with a wired profile:

```
(Instant AP)(config)# wired-port-profile <name>
(Instant AP)(Wired ap profile <name>)# access-rule-name <name>
(Instant AP)(Wired ap profile <name>)# end
(Instant AP)# commit apply
```

Verifying the configuration

To verify the CALEA configuration:

```
(Instant AP)# show calea config
```

To view the tunnel encapsulation statistics:

```
(Instant AP)# show calea statistics
```

Example

To enable CALEA integration:

```
(Instant AP)(config)# calea
(Instant AP)(calea)# ip 192.0.2.7
(Instant AP)(calea)# ip mtu 1500
(Instant AP)(calea)# encapsulation-type GRE
(Instant AP)(calea)# gre-type 255
(Instant AP)(calea)# end

(Instant AP)(config)# wlan access-rule ProfileCalea
(Instant AP)(Access Rule "ProfileCalea")# calea
(Instant AP)(Access Rule "ProfileCalea")# end
(Instant AP)# commit apply

(Instant AP)(config)# wlan ssid-profile Calea-Test
(Instant AP)(SSID Profile"Calea-Test")# enable
(Instant AP)(SSID Profile"Calea-Test")# index 0
```

```
(Instant AP)(SSID Profile"Calea-Test")# type employee
(Instant AP)(SSID Profile"Calea-Test")# essid QA-Calea-Test
(Instant AP)(SSID Profile"Calea-Test")# opmode wpa2-aes
(Instant AP)(SSID Profile"Calea-Test")# max-authentication-failures 0
(Instant AP)(SSID Profile"Calea-Test")# auth-server server1
(Instant AP)(SSID Profile"Calea-Test")# set-role Filter-Id equals 123456 calea-test
(Instant AP)(SSID Profile"Calea-Test")# rf-band 5.0
(Instant AP)(SSID Profile"Calea-Test")# captive-portal disable
(Instant AP)(SSID Profile"Calea-Test")# dtim-period 1
(Instant AP)(SSID Profile"Calea-Test")# inactivity-timeout 1000
(Instant AP)(SSID Profile"Calea-Test")# broadcast-filter none
(Instant AP)(SSID Profile"Calea-Test")# dmo-channel-utilization-threshold 90
(Instant AP)(SSID Profile"Calea-Test")# local-probe-req-thresh 0
(Instant AP)(SSID Profile"Calea-Test")# max-clients-threshold 64
(Instant AP)(SSID Profile"Calea-Test")# end
(Instant AP)(SSID Profile"Calea-Test")# commit apply
```

To verify the configuration:

```
(Instant AP)# show calea config


calea-ip :10.0.0.5
encapsulation-type :gre
gre-type :25944
ip mtu : 150

(Instant AP)# show calea statistics

Rt resolve fail : 0
Dst resolve fail: 0
Alloc failure : 0
Fragged packets : 0
Jumbo packets : 263
Total Tx fail : 0
Total Tx ok : 263
```

This chapter provides information on W-IAP management and monitoring from:

- W-AirWave management server

Managing a W-IAP from W-AirWave

W-AirWave is a powerful tool and easy-to-use network operations system that manages Dell wireless, wired, and remote access networks, as well as wired and wireless infrastructures from a wide range of third-party manufacturers. With its easy-to-use interface, W-AirWave provides real-time monitoring, proactive alerts, historical reporting, and fast, efficient troubleshooting. It also offers tools that manage RF coverage, strengthen wireless security, and demonstrate regulatory compliance.

The W-IAPs communicate with W-AirWave using the HTTPS protocol. This allows a W-AirWave server to be deployed in the cloud across a NAT device, such as a router. The W-AirWave features available in the Instant network are described in the following sections.

Image Management

W-AirWave allows you to manage firmware updates on WLAN devices by defining a minimum acceptable firmware version for each make and model of a device. It remotely distributes the firmware image to the WLAN devices that require updates, and it schedules the firmware updates such that updating is completed without requiring you to manually monitor the devices.

The following models can be used to upgrade the firmware:

- Automatic– In this model, the Virtual Controller periodically checks for newer updates from a configured URL and automatically initiates upgrade of the network.
- Manual– In this model, the user can manually start a firmware upgrade for each Virtual Controller or set the desired firmware preference per group of devices.

W-IAP and Client Monitoring

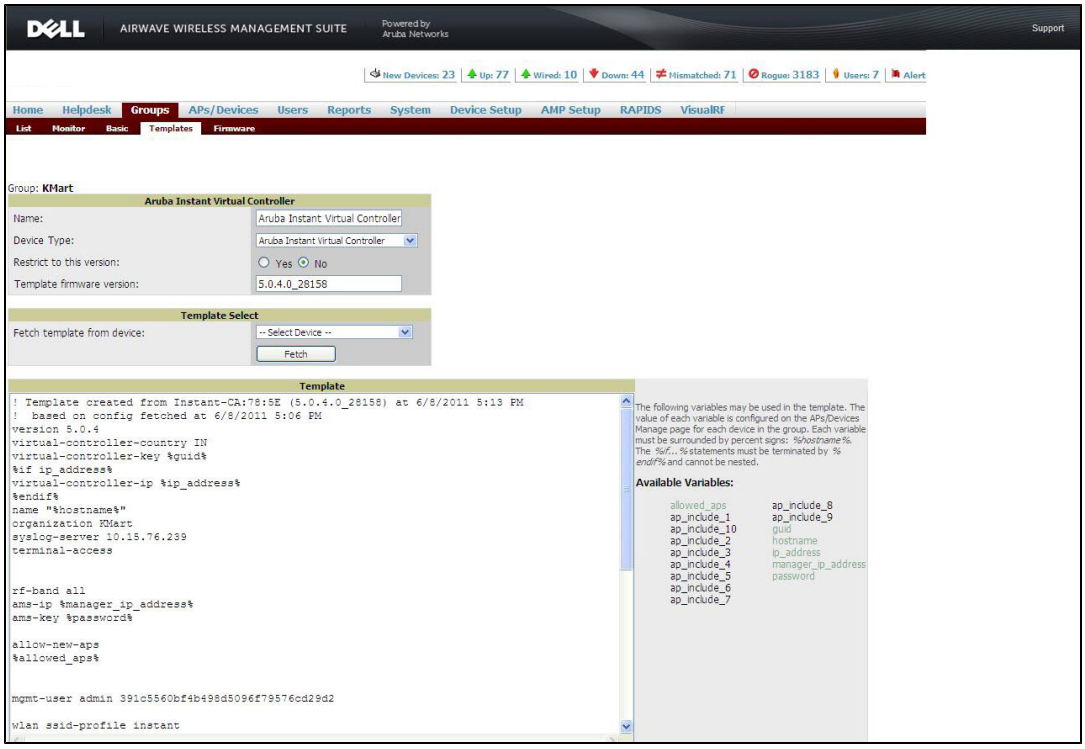
W-AirWave allows you to find any W-IAP or client on the wireless network and to see real-time monitoring views. These monitoring views can be used to aggregate critical information and high-end monitoring information.

In the W-AirWave User Interface (UI), you can select either **Manage Read/Write** or **Monitor-only+Firmware Upgrades** as management modes. When the Management level is set to **Manage Read/Write**, the Instant UI is in read-only mode. If W-AirWave Management Level is set to **Monitor-only+Firmware Upgrades** mode, the Instant UI changes to the read-write mode.

Template-based Configuration

W-AirWave automatically creates a configuration template based on any of the existing W-IAPs, and it applies that template across the network as shown in the following figure. It audits every device on an ongoing basis to ensure that configurations never vary from the enterprise policies. It alerts you whenever a violation is detected and automatically repairs the incorrectly configured devices.

Figure 96 *Template-based Configuration*



Trending Reports

W-AirWave saves up to 14 months of actionable information, including network performance data and user roaming patterns, so you can analyze how network usage and performance trends have changed over time. It also provides detailed capacity reports with which you can plan the capacity and appropriate strategies for your organization.

Intrusion Detection System

W-AirWave provides advanced, rules-based rogue classification. It automatically detects rogue APs irrespective of their location in the network and prevents authorized W-IAPs from being detected as rogue W-IAPs. It tracks and correlates the IDS events to provide a complete picture of network security.

Wireless Intrusion Detection System (WIDS) Event Reporting to W-AirWave

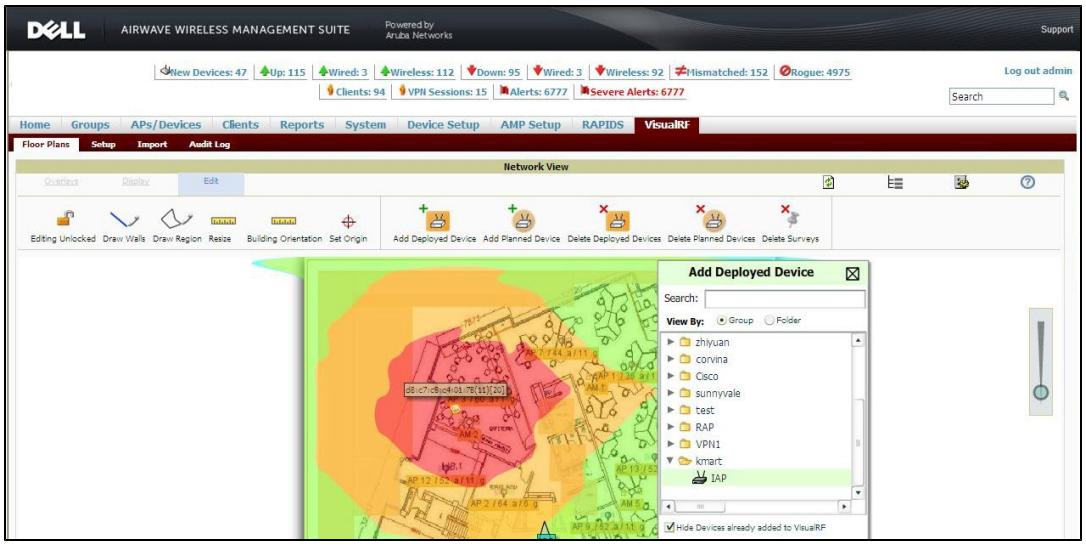
W-AirWave supports Wireless Intrusion Detection System (WIDS) Event Reporting, which is provided by Instant. This includes WIDS classification integration with the RAPIDS (Rogue Access Point Detection Software) module. RAPIDS is a powerful and easy-to-use tool for automatic detection of unauthorized wireless devices. It supports multiple methods of rogue detection and uses authorized wireless APs to report other devices within range.

The WIDS report cites the number of IDS events for devices that have experienced the most instances in the prior 24 hours and provides links to support additional analysis or configuration in response.

RF Visualization Support for Instant

W-AirWave supports RF visualization for Instant. The VisualRF module provides a real-time picture of the actual radio environment of your wireless network and the ability to plan the wireless coverage of new sites. VisualRF uses sophisticated RF fingerprinting to accurately display coverage patterns and calculate the location of every Instant device in range. VisualRF provides graphical access to floor plans, client location, and RF visualization for floors, buildings, and campuses that host your network.

Figure 97 *Adding a W-IAP in VisualRF*



PSK-based and Certificate-based Authentication

On the DHCP server, two formats for option 43 are supported:

- **<organization>,<ams-ip>,<ams-key>**– If you choose this format, the W-IAP authenticates the W-AirWave Management Platform server using the Pre-Shared Key (PSK) login process.
- **<organization>,<ams-domain>**– If you choose this format, the W-IAP resolves the W-AirWave domain name into one or two IP addresses as W-AirWave Primary or W-AirWave Backup, and then W-IAP starts a certificate-based authentication with W-AirWave Management platform server, instead of the PSK login. When the W-AirWave Management platform domain name is used, the W-IAP performs certificate-based authentication with the W-AirWave Management platform server. The W-IAP initiates an SSL connection with the W-AirWave server. The W-AirWave server verifies the signature and public key certificate from the W-IAP. If the signature matches, the W-AirWave responds to the W-IAP with the login request.

Configurable Port for W-IAP and W-AirWave Management Server Communication

You can now customize the port number of the W-AirWave management server through the **server_host:server_port** format, for example, **amp.aruba.com:4343**.

Configuring Organization String

The Organization string is a set of colon-separated strings created by the W-AirWave administrator to accurately represent the deployment of each W-IAP. This string is defined by the installation personnel on the site.

You can use any of the following strings:

- AMP Role– "Org Admin" (initially disabled)
- AMP User– "Org Admin" (assigned to the role "Org Admin")
- Folder– "Org" (under the Top folder in AMP)
- Configuration Group– "Org"

You can also assign additional strings to create a hierarchy of sub folders under the folder named "Org". For example:

  - subfolder1 for a folder under the "Org" folder
  - subfolder2 for a folder under subfolder1

Shared Key

The Shared Secret key is an optional field used by the administrator to manually authorize the first Virtual Controller for an organization. Any string is acceptable.

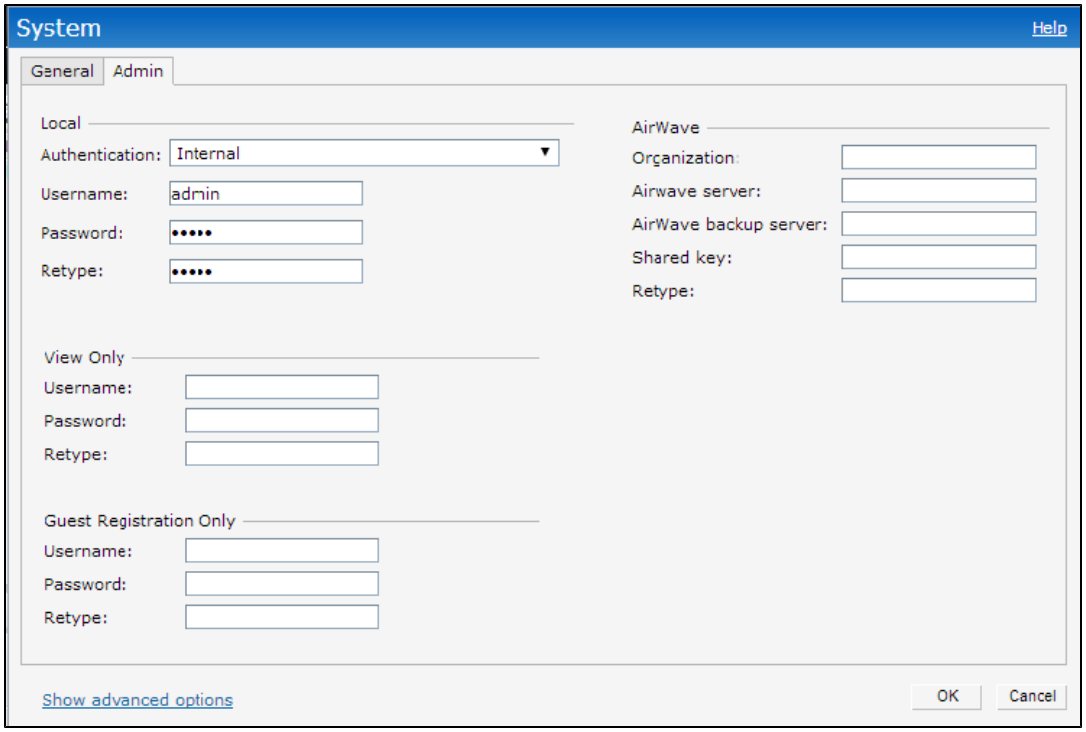
Configuring W-AirWave Information

You can configure W-AirWave information using the Instant UI or CLI.

In the Instant UI

1. Click the W-AirWave **Set Up Now** link in the bottom-middle region of the main window. The **System** window is displayed with the W-AirWave parameters in the **Admin** tab.

Figure 98 *Configuring W-AirWave*



2. Enter the name of your organization in the **Organization** name text box. The name defined for organization is displayed under the **Groups** tab in the W-AirWave user interface.
3. Enter the IP address or domain name of the W-AirWave server in the **AirWave server** text box.
4. Enter the IP address or domain name of a backup W-AirWave server in the **AirWave backup server** text box. The backup server provides connectivity when the primary server is down. If the W-IAP cannot send data to the primary server, the Virtual Controller switches to the backup server automatically.
5. Enter the shared key in the **Shared key** text box and reconfirm. This shared key is used for configuring the first AP in the Instant network.
6. Click **OK**.

In the CLI

To configure W-AirWave information in Instant:

```
(Instant AP)(config)# organization <name>
(Instant AP)(config)# ams-ip <IP-address or domain name>
(Instant AP)(config)# ams-backup-ip <IP-address or domain name>
(Instant AP)(config)# ams-key <key>
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Configuring for W-AirWave Discovery through DHCP

The W-AirWave can be discovered through DHCP server. You can configure this only if W-AirWave was not configured earlier or if you have deleted the precedent configuration.

On the DHCP server, the format for option 60 is " **InstantAP**", and the two formats for option 43 are "**<organization>,<ams-ip>,<ams-key>**" and "**<organization>,<ams-domain>**" .

If you use the **<organization>,<ams-ip>,<ams-key>** format, the PSK-based authentication is used to access the W-AirWave Management Platform server.

If you use the **<organization>,<ams-domain>** format, the W-IAP resolves the domain name into two IP address as W-AirWave Primary W-AirWave Backup, and then W-IAP starts a certificate-based authentication with W-AirWave Management platform server, instead of the PSK login.

NOTE

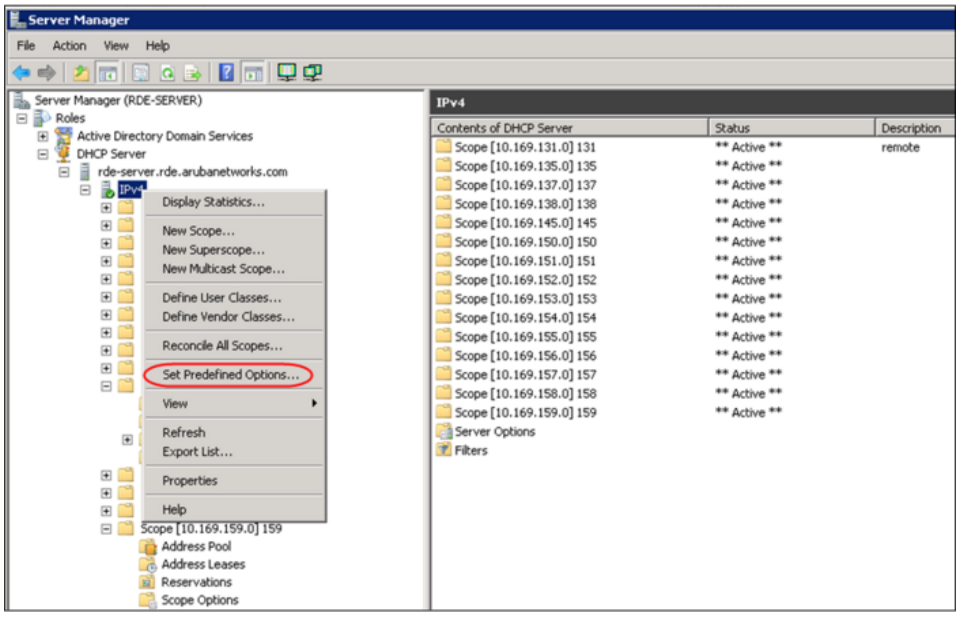
For option 43, when you choose to enter the domain name, the IP address and key are not available.

Standard DHCP option 60 and 43 on Windows Server 2008

In networks that are not using DHCP option 60 and 43, it is easy to use the standard DHCP options 60 and 43 for an AP or W-IAP. For APs, these options can be used to indicate the master controller or the local controller. For W-IAPs, these options can be used to define the W-AirWave IP, group, password, and domain name.

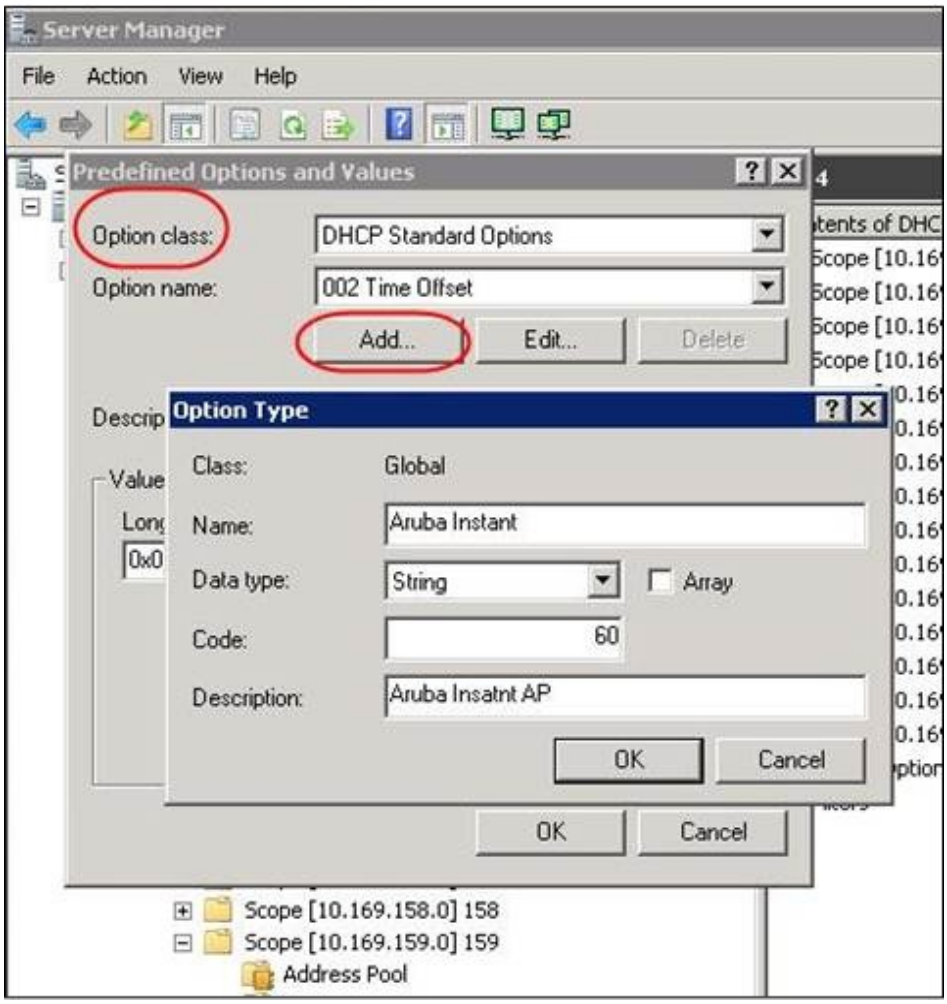
1. From a server running Windows Server 2008 navigate to **Server Manager** > **Roles** > **DHCP sever** >**domain DHCP Server** > **IPv4**.
2. Right-click **IPv4** and select **Set Predefined Options.**

Figure 99 *Instant and DHCP options for W-AirWave: Set Predefined Options*



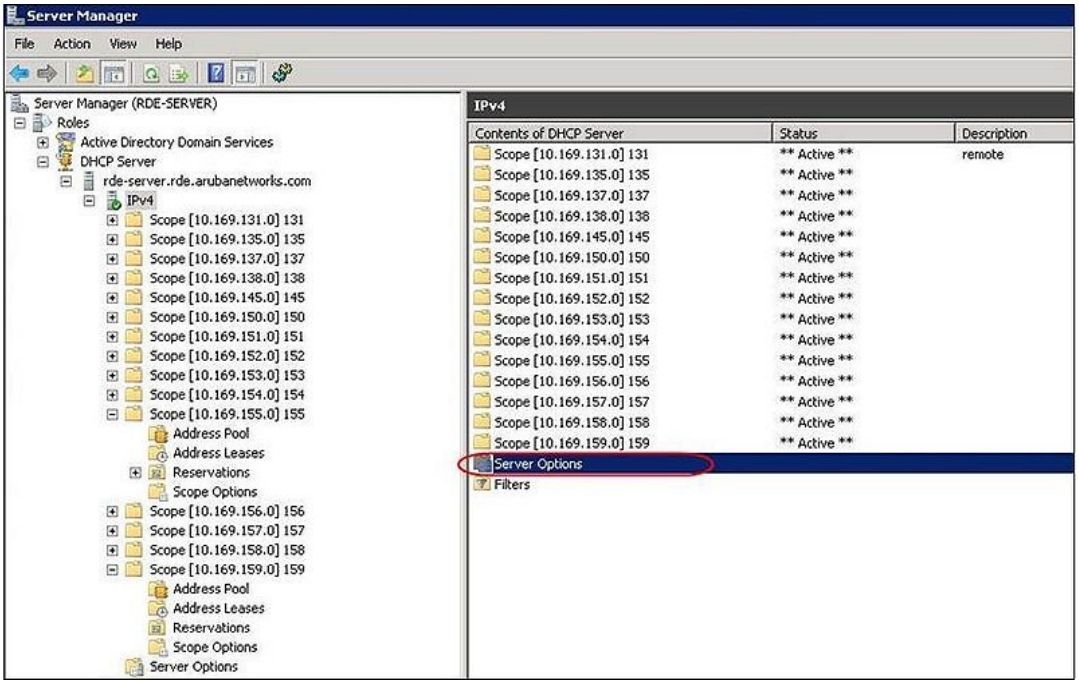
3. Select **DHCP Standard Options** in the **Option class** drop-down list and then click **Add**.
4. Enter the following information:
   - Name– Instant
   - Data Type– String
   - Code–60
   - Description–Instant AP

Figure 100 *Instant and DHCP options for W-AirWave: Predefined Options and Values*



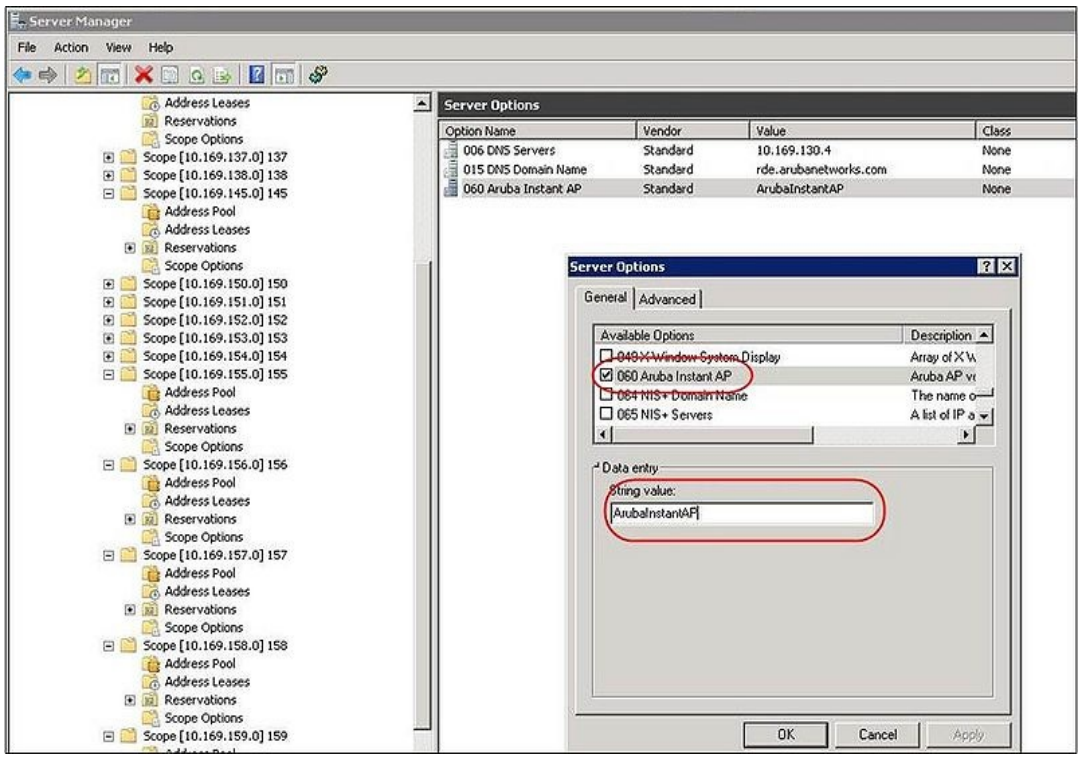
5. Navigate to **Server Manager** and select **Server Options** in the **IPv4** window. (This sets the value globally. Use options on a per-scope basis to override the global options.)
6. Right-click **Server Options** and select the configuration options.

Figure 101 *Instant and DHCP options for W-AirWave: Server Options*



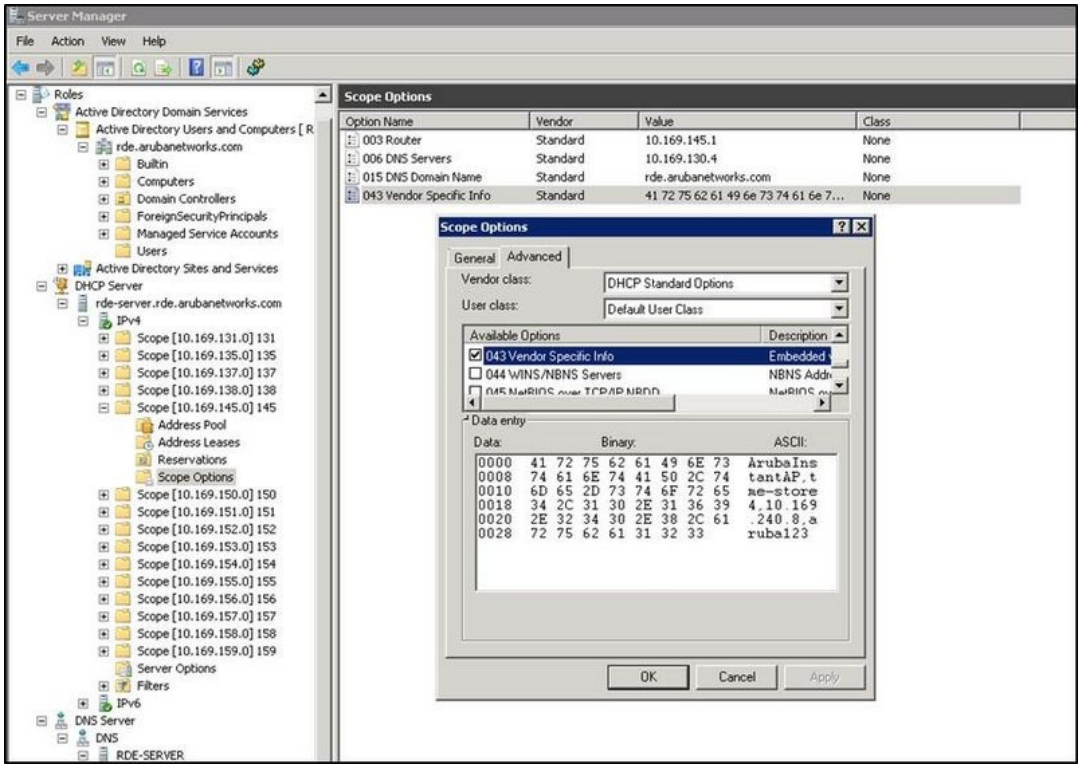
7. Select **060 Dell Instant AP** in the **Server Options** window and enter **DellInstantAP** in the String Value.

Figure 102 *Instant and DHCP options for W-AirWave—060 W-IAP in Server Options*



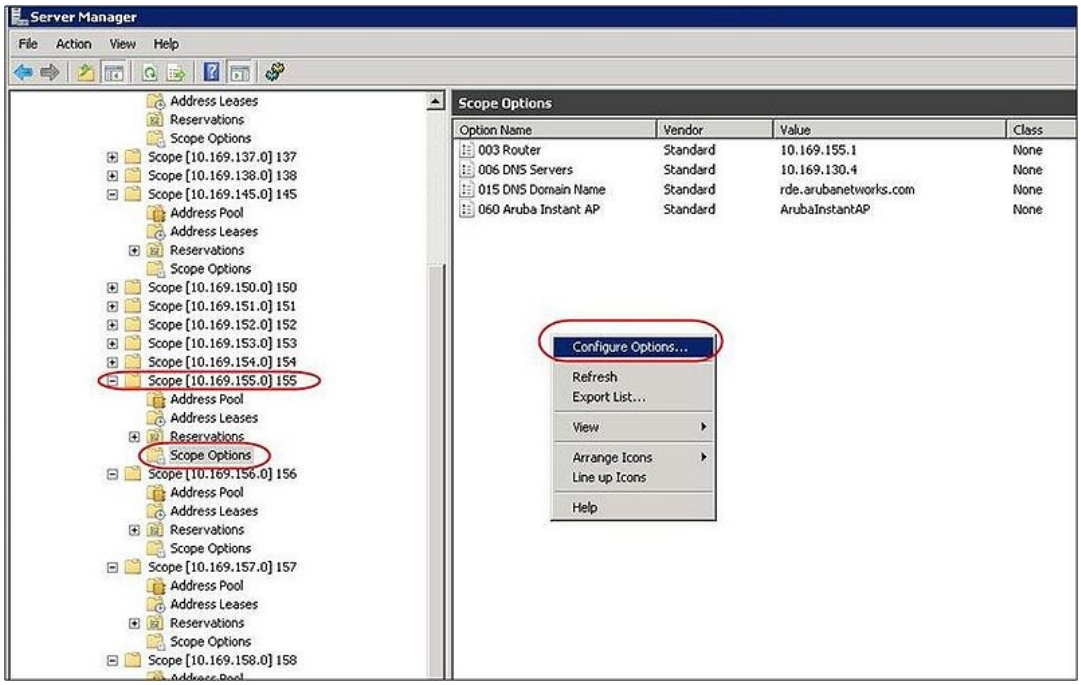
8. Select **043 Vendor Specific Info** and enter a value for either of the following in ASCII field:
   - **airwave-orgn, airwave-ip, airwave-key**; for example: Dell,192.0.2.20, 12344567
   - **airwave-orgn, airwave-domain**; for example: Dell, dell.support.com

Figure 103 *Instant and DHCP options for W-AirWave— 043 Vendor Specific Info*



This creates a DHCP option 60 and 43 on a global basis. You can do the same on a per-scope basis. The per-scope option overrides the global option.

Figure 104 *Instant and DHCP options for W-AirWave: Scope Options*



Alternate Method for Defining Vendor-Specific DHCP Options

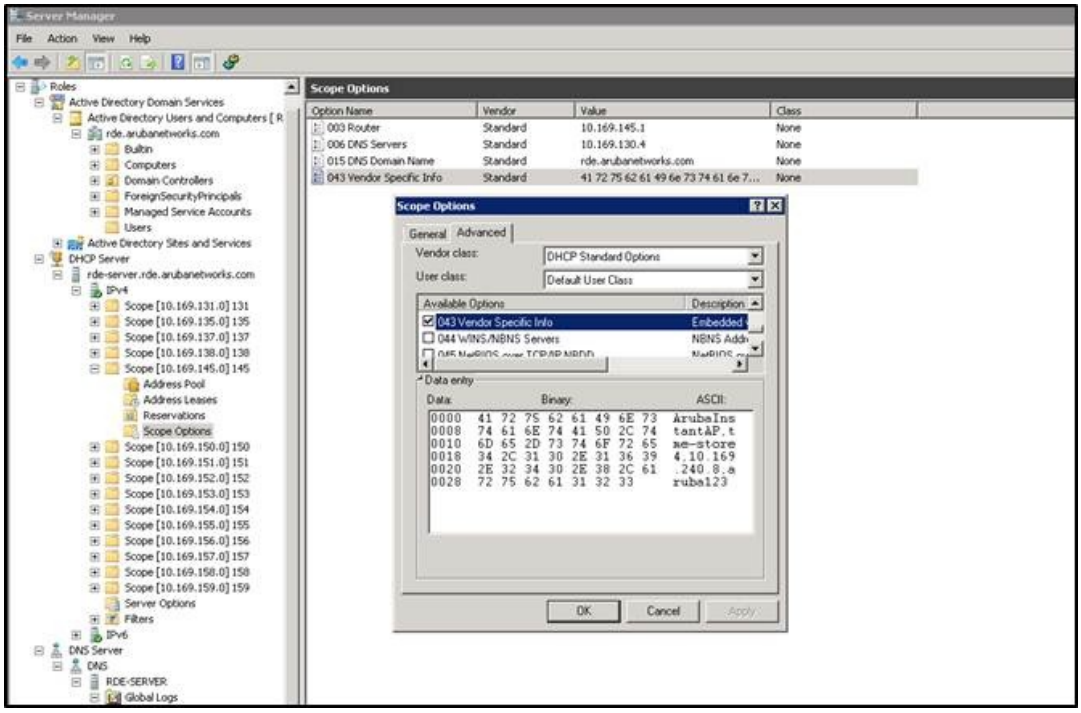
This section describes how to add vendor-specific DHCP options for Instant APs in a network that already uses DHCP options 60 and 43 for other services. Some networks use DHCP standard options 60 and 43 to provide the DHCP clients information about certain services such as PXE. In such an environment, the standard DHCP options 60 and 43 cannot be used for W-IAPs.

This method describes how to set up a DHCP server to send option 43 with W-AirWave information to the W-IAP. This section assumes that option 43 is sent per scope, because option 60 is being shared by other devices as well.

The DHCP scope must be specific to Instant, and the PXE devices that use options 60 and 43 must not connect to the subnet defined by this scope. This is because you can specify only one option 43 for a scope, and if other devices that use option 43 connect to this subnet, they are presented with the information specific to the W-IAP.

1. In server 2008, navigate to **Server Manager > Roles > DHCP Server > Domain DHCP Server > IPv4**.
2. Select a scope (subnet). Scope (10.169.145.0)145 is selected in the example shown in the figure below.
3. Right-click and select **Advanced,** and then specify the following options:
   - Vendor class– DHCP Standard Options
   - User class– Default User Class
   - Available options– Select 043 Vendor-Specific Info
   - String Value– DellInstantAP, tme-store4, 10.169.240.8, Dell123 (which is the AP description, organization string, W-AirWave IP address or domain name, Pre-shared key, for W-AirWave)

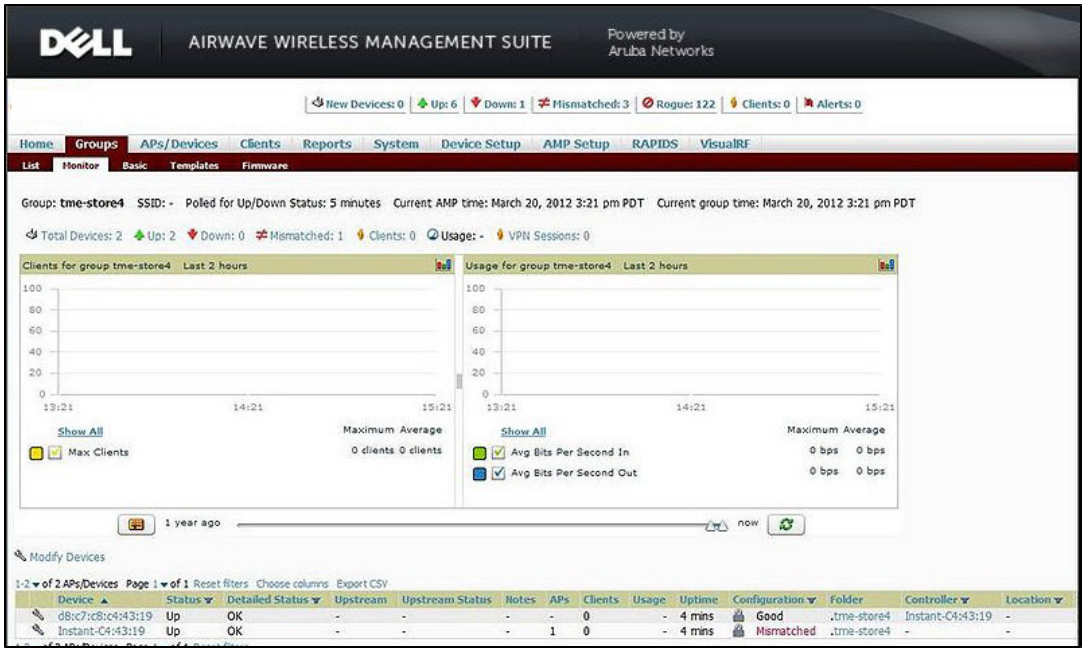
Figure 105 *Vendor Specific DHCP options*



Upon completion, the W-IAP shows up as a new device in W-AirWave, and a new group called **tme-store4** is created. Navigate to **APs/Devices > New > Group** to view this group.

Figure 106 *W-AirWave — New Group*

Figure 107 *W-AirWave —Monitor*



This chapter provides the following information:

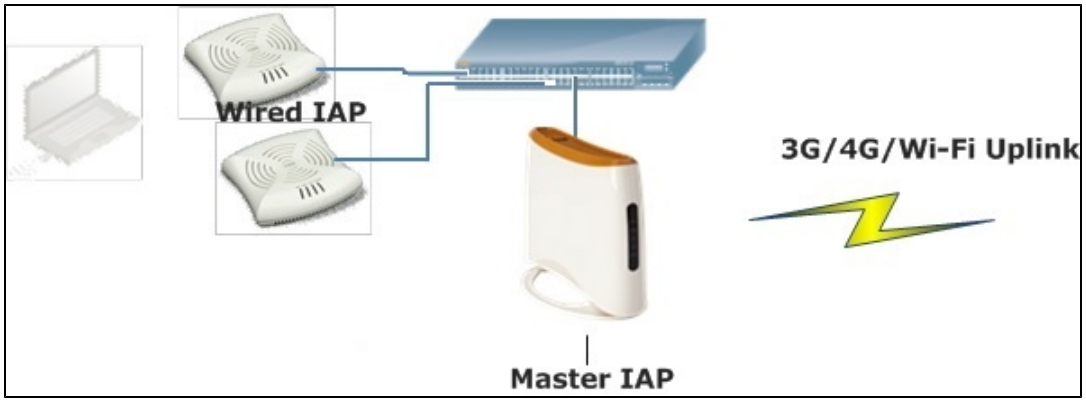
- Uplink Interfaces on page 285
- Ethernet Uplink on page 285
- Cellular Uplink on page 287
- Wi-Fi Uplink on page 291
- Uplink Preferences and Switching on page 292

Uplink Interfaces

Instant network supports Ethernet, 3G and 4G USB modems, and the Wi-Fi uplink to provide access to the corporate Instant network. The 3G/4G USB modems and the Wi-Fi uplink can be used to extend the connectivity to places where an Ethernet uplink cannot be configured. It also provides a reliable backup link for the Ethernet based Instant network.

The following figure illustrates a scenario in which the W-IAPs join the Virtual Controller as slave W-IAPs through a wired or mesh Wi-Fi uplink:

Figure 108 *Uplink Types*



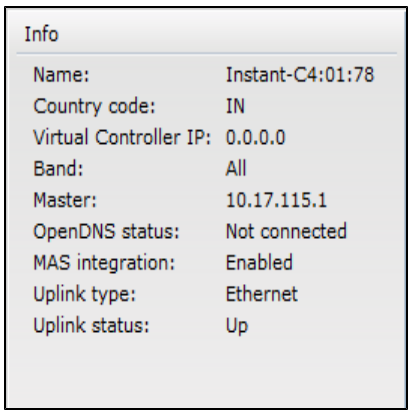
The following types of uplinks are supported on Instant:

- Ethernet Uplink
- Cellular Uplink
- Wi-Fi Uplink

Ethernet Uplink

The Ethernet 0 port on a W-IAP is enabled as an uplink port by default. You can view the type of uplink and the status of the uplink in the Instant in the **Info** tab on selecting a client.

Figure 109 *Uplink Status*



Ethernet uplink supports the following types of configuration in this Instant release.

- PPPoE
- DHCP
- Static IP

You can use PPPoE for your uplink connectivity in both W-IAP and IAP-VPN deployments. PPPoE is supported only in a single AP deployment.

NOTE

Uplink redundancy with the PPPoE link is not supported.

When the Ethernet link is up, it is used as a PPPoE or DHCP uplink. After the PPPoE settings are configured, PPPoE has the highest priority for the uplink connections. The W-IAP can establish a PPPoE session with a PPPoE server at the ISP and get authenticated using Password Authentication Protocol (PAP) or the Challenge Handshake Authentication Protocol (CHAP). Depending upon the request from the PPPoE server, either the PAP or the CHAP credentials are used for authentication. After configuring PPPoE, reboot the W-IAP for the configuration to affect. The PPPoE connection is dialed after the AP comes up. The PPPoE configuration is checked during W-IAP boot and if the configuration is correct, Ethernet is used for the uplink connection.

NOTE

When PPPoE is used, do not configure Dynamic RADIUS Proxy and IP address of the Virtual Controller. An SSID created with default VLAN is not supported with PPPoE uplink.

You can also configure an alternate Ethernet uplink to enable uplink failover when an Ethernet port fails.

Configuring PPPoE Uplink Profile

You can configure PPPOE settings from the Instant UI or CLI.

In the Instant UI

1. Click the **System** link at the top right corner of the Instant main window. The **System** window is displayed.
2. Click the **Show advanced options** link. The advanced options are displayed.
3. In the **Uplink** tab, perform the following steps in the **PPPoE** section:
   a. Enter the **PPPoE service name** provided by your service provider in the **Service name** field.
   b. In the **CHAP secret** and **Retype** fields, enter the secret key used for Challenge Handshake Authentication Protocol (CHAP) authentication. You can use a maximum of 34 characters for the CHAP secret key.
   c. Enter the user name for the PPPoE connection in the **User** field.
   d. In the **Password** and **Retype** fields, enter a password for the PPPoE connection and confirm it.

4. To set a local interface for the PPPoE uplink connections, select a value from the **Local interface** drop-down list. The selected DHCP scope will be used as a local interface on the PPPoE interface and the Local,L3 DHCP gateway IP address as its local IP address. When configured, the local interface acts as an unnumbered PPPoE interface and allows the entire Local,L3 DHCP subnet to be allocated to clients.

The options in the **Local interface** drop-down list are displayed only if a Local,L3 DHCP scope is configured on the W-IAP.

5. Click **OK**.
6. Reboot the W-IAP for the configuration to affect.

In the CLI

To configure a PPPoE uplink connection:

```
(Instant AP)(config) # pppoe-uplink-profile
(Instant AP)(pppoe-uplink-profile)# pppoe-svcname <service-name>
(Instant AP)(pppoe-uplink-profile)# pppoe-username <username>
(Instant AP)(pppoe-uplink-profile)# pppoe-passwd <password>
(Instant AP)(pppoe-uplink-profile)# pppoe-chapsecret <password>
(Instant AP)(pppoe-uplink-profile)# pppoe-unnumbered-local-l3-dhcp-profile <dhcp-profile>
(Instant AP)(pppoe-uplink-profile)# end
(Instant AP)# commit apply
```

To view the PPPoE configuration:

```
(Instant AP)# show pppoe config

PPPoE Configuration
-------------------
Type Value
---- -----
User testUser
Password 3c28ec1b82d3eef0e65371da2f39c4d49803e5b2bc88be0c
Service name internet03
CHAP secret 8e87644deda9364100719e017f88ebce
Unnumbered dhcp profile dhcpProfile1
```

To view the PPPoE status:

```
(Instant AP)# show pppoe status

pppoe uplink state:Suppressed.
```

Cellular Uplink

Instant supports the use of 3G and 4G USB modems to provide the Internet backhaul to an Instant network. The 3G or 4G USB modems can be used to extend client connectivity to places where an Ethernet uplink cannot be configured. This enables the W-IAPs to automatically choose the available network in a specific region.

The 3G and 4G LTE USB modems can be provisioned on W-IAP3WN/3WNP, W-IAP108/109, and W-IAP155/155P.

The following 3G modems are supported:

- USBConnect 881 (Sierra 881U)
- Quicksilver (Globetrotter ICON 322)
- UM100C (UTstarcom)
- Icon 452

- Aircard 250U (Sierra)
- USB 598 (Sierra)
- U300 (Franklin wireless)
- U301 (Franklin wireless)
- USB U760 for Virgin (Novatel)
- USB U720 (Novatel/Qualcomm)
- UM175 (Pantech)
- UM150 (Pantech)
- UMW190(Pantech)
- SXC-1080 (Qualcomm)
- Globetrotter ICON 225
- UMG181
- NTT DoCoMo L-05A (LG FOMA L05A)
- NTT DoCoMo L-02A
- ZTE WCDMA Technologies MSM (MF668?)
- Fivespot (ZTE)
- c-motech CNU-600
- ZTE AC2736
- SEC-8089 (EpiValley)
- Nokia CS-10
- NTT DoCoMo L-08C (LG)
- NTT DoCoMo L-02C (LG)
- Novatel MC545
- Huawei E220 for Movistar in Spain
- Huawei E180 for Movistar in Spain
- ZTE-MF820
- Huawei E173s-1
- Sierra 320
- Longcheer WM72
- U600 (3G mode)
- Sierra USB-306 (HK CLS/1010 (HK))
- Sierra 306/308 (Telstra (Aus))
- Sierra 503 PCIe (Telstra (Aus))
- Sierra 312 (Telstra (Aus))
- Aircard USB 308 (AT&T's Shockwave)
- Compass 597(Sierra) (Sprint)
- U597 (Sierra) (Verizon)
- Tstick C597(Sierra) (Telecom(NZ))
- Ovation U727 (Novatel) (Sprint)
- USB U727 (Novatel) (Verizon)
- USB U760 (Novatel) (Sprint)
- USB U760 (Novatel) (Verizon)

- Novatel MiFi 2200 (Verizon Mifi 2200)
- Huawei E272, E170, E220 (ATT)
- Huawei E169, E180,E220,E272 (Vodafone/SmarTone (HK))
- Huawei E160 (O2(UK))
- Huawei E160 (SFR (France))
- Huawei E220 (NZ and JP)
- Huawei E176G (Telstra (Aus))
- Huawei E1553, E176 (3/HUTCH (Aus))
- Huawei K4505 (Vodafone/SmarTone (HK))
- Huawei K4505 (Vodafone (UK))
- ZTE MF656 (Netcom (norway))
- ZTE MF636 (HK CSL/1010)
- ZTE MF633/MF636 (Telstra (Aus))
- ZTE MF637 (Orange in Israel)
- Huawei E180, E1692,E1762 (Optus (Aus))
- Huawei E1731 (Airtel-3G (India))
- Huawei E3765 (Vodafone (Aus))
- Huawei E3765 (T-Mobile (Germany)
- Huawei E1552 (SingTel)
- Huawei E1750 (T-Mobile (Germany))
- UGM 1831 (TMobile)
- Huawei D33HW (EMOBILE(Japan))
- Huawei GD01 (EMOBILE(Japan))
- Huawei EC150 (Reliance NetConnect+ (India))
- KDDI DATA07(Huawei) (KDDI (Japan))
- Huawei E353 (China Unicom)
- Huawei EC167 (China Telecom)
- Huawei E367 (Vodafone (UK))
- Huawei E352s-5 (T-Mobile (Germany))
- Huawei K4505 (Vodafone/SmarTone (HK))
- Huawei K4505 (Vodafone (UK))
- ZTE MF656 (Netcom (norway))
- ZTE MF636 (HK CSL/1010)
- ZTE MF633/MF636 (Telstra (Aus))
- ZTE MF637 (Orange in Israel)
- Huawei E180, E1692,E1762 (Optus (Aus))
- Huawei E1731 (Airtel-3G (India))
- Huawei E3765 (Vodafone (Aus))
- Huawei E3765 (T-Mobile (Germany)
- Huawei E1552 (SingTel)
- Huawei E1750 (T-Mobile (Germany))
- UGM 1831 (TMobile)

- Huawei D33HW (EMOBILE(Japan))
- Huawei GD01 (EMOBILE(Japan))
- Huawei EC150 (Reliance NetConnect+ (India))
- KDDI DATA07(Huawei) (KDDI (Japan))
- Huawei E353 (China Unicom)
- Huawei EC167 (China Telecom)
- Huawei E367 (Vodafone (UK))
- Huawei E352s-5 (T-Mobile (Germany))
- Huawei D41HW
- ZTE AC2726

The following table lists the supported 4G modems.

- Netgear U340
- Netgear Aircard 341u
- Fraklin Wireless u770
- Huawei 3276s-150
- MC551L
- Pantech UML295
- Pantech UML290

In the 6.4.0.2-4.1 release, all modems are detected automatically by the W-IAP.

When UML290 runs in auto detect mode, the modem can switch from 4G network to 3G network or vice-versa based on the signal strength. To configure the UML290 for the 3G network only, manually set the USB type to **pantech-3g**. To configure the UML290 for the 4G network only, manually set the 4G USB type to **pantech-lte**.

Configuring Cellular Uplink Profiles

You can configure 3G or 4G uplinks using the Instant UI or CLI.

In the Instant UI

1. Click the **System** link at the upper right corner of the Instant main window. The **System** window is displayed.
2. In the **System** window, click the **show advanced settings** link. The advanced options are displayed.
3. Click the **Uplink** tab.
4. To configure a 3G or 4G uplink manually, select the **Country** and **ISP**.
5. Click **OK**.
6. Reboot the W-IAP for changes to affect.

In the CLI

To configure 3G/4G uplink manually:

```
(Instant AP)(config) # cellular-uplink-profile
(Instant AP)(cellular-uplink-profile)# usb-type <3G-usb-type>
(Instant AP)(cellular-uplink-profile)# 4g-usb-type <4g-usb>
(Instant AP)(cellular-uplink-profile)# modem-country <country>
(Instant AP)(cellular-uplink-profile)# modem-isp <service-provider-name>
(Instant AP)(cellular-uplink-profile)# usb-auth-type <usb-authentication_type>
(Instant AP)(cellular-uplink-profile)# usb-user <username>
(Instant AP)(cellular-uplink-profile)# usb-passwd <password>
(Instant AP)(cellular-uplink-profile)# usb-dev <device-ID>
(Instant AP)(cellular-uplink-profile)# usb-tty <tty-port>
(Instant AP)(cellular-uplink-profile)# usb-init <Initialization-parameter>
```

```
(Instant AP)(cellular-uplink-profile)# usb-dial <dial-parameter>
(Instant AP)(cellular-uplink-profile)# usb-modeswitch <usb-modem>
(Instant AP)(cellular-uplink-profile)# end
(Instant AP)# commit apply
```

To switch a modem from the storage mode to modem mode:

```
(Instant AP)(config)# cellular-uplink-profile
(Instant AP)(cellular-uplink-profile)# usb-modeswitch <usb-modem>
```

To view the cellular configuration:

```
(Instant AP)# show cellular config
```

Wi-Fi Uplink

The Wi-Fi uplink is supported for all the W-IAP models, but only the master W-IAP uses this uplink. The Wi-Fi allows uplink to open, PSK-CCMP, and PSK-TKIP SSIDs.

- For single radio W-IAPs, the radio serves wireless clients and the Wi-Fi uplink.
- For dual radio W-IAPs, both radios can be used to serve clients but only one of them can be used for the Wi-Fi uplink.

When the Wi-Fi uplink is in use, the client IP is assigned by the internal DHCP server.

Configuring a Wi-Fi Uplink Profile

The following configuration conditions apply to the Wi-Fi uplink:

- To bind or unbind the Wi-Fi uplink on the 5 GHz band, reboot the W-IAP.
- If the Wi-Fi uplink is used on the 5 GHz band, mesh is disabled. The two links are mutually exclusive.
- For W-IAPs to connect to an ArubaOS based WLAN using Wi-Fi uplink, the controller must run ArubaOS 6.2.1.0 or later.

To provision a with the Wi-Fi Uplink, complete the following steps:

1. If you are configuring a Wi-Fi uplink after restoring factory settings on a W-IAP, connect the W-IAP to an Ethernet cable to allow the W-IAP to get the IP address. Otherwise, go to step 2.
2. Click the **System** link at the top right corner of the Instant main window. The **System** window is displayed.
3. Click the **Show advanced options** link. The advanced options are displayed.
4. Click the **Uplink** tab.
5. Under Wi-Fi, enter the name of the wireless network that is used for the Wi-Fi uplink in the **Name (SSID)** text box.
6. Select the type of key for uplink encryption and authentication from the **Key management** drop-down list. If the uplink wireless router uses mixed encryption, WPA-2 is recommended for the Wi-Fi uplink.
7. From the **band** drop-down list. Select the band in which the Virtual Controller currently operates. The following options are available:
   - 2.4 GHz (default)
   - 5 GHz
8. Select a passphrase format from the **Passphrase format** drop-down list. The following options are available:
   - 8 - 63 alphanumeric characters
   - 64 hexadecimal characters

Ensure that the hexadecimal password string is exactly 64 digits in length.

9. Enter a pre-shared key (PSK) passphrase in the **Passphrase** text box and click **OK**.

You can view the W-Fi configuration and uplink status in the CLI. To view the configuration status in the CLI:

```
(Instant AP)# show wifi-uplink status
configured :NO

(Instant AP)# show wifi-uplink config

ESSID :
Cipher Suite :
Passphrase :
Band :

(Instant AP)# show wifi-uplink auth log

----------------------------------------------------------------------
wifi uplink auth configuration:
----------------------------------------------------------------------
----------------------------------------------------------------------
wifi uplink auth log:
----------------------------------------------------------------------
[1116]2000-01-01 00:00:45.625: Global control interface '/tmp/supp_gbl'
```

Uplink Preferences and Switching

This topic describes the following procedures:

- Enforcing Uplinks on page 292
- Setting an Uplink Priority on page 293
- Enabling Uplink Preemption on page 293
- Switching Uplinks Based on VPN and Internet Availability on page 294
- Viewing Uplink Status and Configuration on page 295

Enforcing Uplinks

The following configuration conditions apply to the uplink enforcement:

- When an uplink is enforced, the W-IAP uses the specified uplink regardless of uplink preemption configuration and the current uplink status.
- When an uplink is enforced and multiple Ethernet ports are configured and uplink is enabled on the wired profiles, the W-IAP tries to find an alternate Ethernet link based on the priority configured.
- When no uplink is enforced and preemption is not enabled, and if the current uplink fails, the W-IAP tries to find an available uplink based on the priority configured.
- When no uplink is enforced and preemption is enabled, and if the current uplink fails, the W-IAP tries to find an available uplink based on the priority configured. If current uplink is active, the W-IAP periodically tries to use a higher priority uplink and switches to the higher priority uplink even if the current uplink is active.

You can enforce a specific uplink on a W-IAP by using the Instant UI or CLI.

In the Instant UI

To enforce an uplink:

1. Click the **System** > **show advanced settings** > **Uplink**. The **Uplink** tab contents are displayed.
2. Under **Uplink Management**, select the type of uplink from the **Enforce Uplink** drop-down list. If Ethernet uplink is selected, the **Port** field is displayed.
3. Specify the Ethernet interface port number.

4. Click **OK**. The selected uplink is enforced on the W-IAP.

In the CLI

To enforce an uplink:

```
(Instant AP)(config)# uplink
(Instant AP)(uplink)# enforce {cellular|ethernet|wifi|none}
(Instant AP)(uplink)# end
(Instant AP)# commit apply
```

Setting an Uplink Priority

You can set an uplink priority by using the Instant UI or CLI.

In the Instant UI

1. Click the **System** > **show advanced settings** > **Uplink**. The **Uplink** tab contents are displayed.
2. Under **Uplink Priority List**, select the uplink, and click the icons at the bottom of the **Uplink Priority List** section, to increase or decrease the priority. By default, the Eth0 uplink is set as a high priority uplink.
3. Click **OK**. The selected uplink is prioritized over other uplinks.

In the CLI

To set an uplink priority:

```
(Instant AP)(config)# uplink
(Instant AP)(uplink)# uplink-priority {cellular <priority> | ethernet <priority>|[port
<Interface-number> <priority>]|wifi <priority>}
(Instant AP)(uplink)# end
(Instant AP)# commit apply
```

For example, to set a priority for Ethernet uplink:

```
(Instant AP)(uplink)# uplink-priority ethernet port 0 1
(Instant AP)(uplink)# end
(Instant AP)# commit apply
```

Enabling Uplink Preemption

The following configuration conditions apply to uplink preemption:

- Preemption can be enabled only when no uplink is enforced.
- When preemption is disabled and the current uplink goes down, the W-IAP tries to find an available uplink based on the uplink priority configuration.
- When preemption is enabled and if the current uplink is active, the W-IAP periodically tries to use a higher priority uplink, and switches to a higher priority uplink even if the current uplink is active.

You can enable uplink preemption using Instant UI or CLI.

In the Instant UI

1. Click the **System** > **show advanced settings** > **Uplink**. The **Uplink** tab contents are displayed.
2. Under **Uplink Management**, ensure that the **Enforce Uplink** is set to none.
3. Select **Enabled** from the **Pre-emption** drop-down list.
4. Click **OK**.

In the CLI

To enable uplink preemption:

```
(Instant AP)(config)# uplink
(Instant AP)(uplink)# preemption
```

```
(Instant AP)(uplink)# end
(Instant AP)# commit apply
```

Switching Uplinks Based on VPN and Internet Availability

The default priority for uplink switchover is Ethernet and then 3G/4G. The W-IAP can switch to the lower priority uplink if the current uplink is down.

Switching Uplinks Based on VPN Status

Instant supports switching uplinks based on the VPN status when deploying multiple uplinks (Ethernet, 3G/4G, and Wi-Fi). When VPN is used with multiple backhaul options, the W-IAP switches to an uplink connection based on the VPN connection status, instead of only using the Ethernet or the physical backhaul link.

The following configuration conditions apply to uplink switching:

- If the current uplink is Ethernet and the VPN connection is down, the W-IAP tries to reconnect to VPN. The retry time depends on the fast failover configuration and the primary or backup VPN tunnel. If this fails, the W-IAP waits for the VPN failover timeout and selects a different uplink such as 3G/4G or Wi-Fi.
- If the current uplink is 3G or Wi-Fi, and Ethernet has a physical link, the W-IAP periodically suspends user traffic to try and connect to the VPN on the Ethernet. If the W-IAP succeeds, the W-IAP switches to Ethernet. If the W-IAP does not succeed, it restores the VPN connection to the current uplink.

Uplink switching based on VPN status is automatically enabled if VPN is configured on the W-IAP. However, you can specify the duration in **VPN failover timeout** field to wait for an uplink switch. By default, this duration is set to 180 seconds. The W-IAP monitors the VPN status and when the VPN connection is not available for 3 minutes, the uplink switches to another available connection (if a low priority uplink is detected and the uplink preference is set to none). When **VPN failover timeout** is set to 0, uplink does not switch over.

When uplink switching based on the Internet availability is enabled, the uplink switching based on VPN failover is automatically disabled.

Switching Uplinks Based on Internet Availability

You can configure Instant to switch uplinks based on Internet availability.

When the uplink switchover based on Internet availability is enabled, the W-IAP continuously sends ICMP packets to some well-known Internet servers. If the request is timed out due to a bad uplink connection or uplink interface failure, and the public Internet is not reachable from the current uplink, the W-IAP switches to a different connection.

You can set preferences for uplink switching using the Instant UI and CLI.

In the Instant UI

To configure uplink switching:

1. Click the **System** > **show advanced settings** > **Uplink**. The **Uplink** tab contents are displayed.
2. Under **Uplink Management**, configure the following parameters:
   - **VPN failover timeout** – To configure uplink switching based on VPN status, specify the duration to wait for an uplink switch. The default duration is set to 180 seconds.
   - **Internet failover** – To configure uplink switching based on Internet availability, perform the following steps:
     a. Select **Enabled** from the **Internet failover** drop-down list.
     b. Specify the required values for the following fields:
        - **Max allowed test packet loss**– The maximum number of ICMP test packets that are allowed to be lost to determine if the W-IAP must switch to a different uplink connection. You can specify a value within the range of 1–1000.

- **Secs between test packets**– The frequency at which ICMP test packets are sent.You can specify a value within the range of 1–3600 seconds.
- **Internet check time**– Internet check timeout is the duration for the test packet timeout. You can specify a value within the range of 0–3600 seconds and the default value is 10 seconds.

c. Click **OK**.

When **Internet failover** is enabled, the W-IAP ignores the VPN status, although uplink switching based on VPN status is enabled.

In the CLI

To enable uplink switching based on VPN status:

```
(Instant AP)(config)# uplink
(Instant AP)(uplink)# failover-vpn-timeout <seconds>
(Instant AP)(uplink)# end
(Instant AP)# commit apply
```

To enable uplink switching based on Internet availability:

```
(Instant AP)(config)# uplink
(Instant AP)(uplink)# failover-internet
(Instant AP)(uplink)# failover-internet-pkt-lost-cnt <count>
(Instant AP)(uplink)# failover-internet-pkt-send-freq <frequency>
(Instant AP)(uplink)# end
(Instant AP)# commit apply
```

Viewing Uplink Status and Configuration

To view the uplink status and configuration in the CLI:

```
Instant Access Point# show uplink status

Uplink preemption :enable
Uplink enforce :none
Ethernet uplink bond0 :DHCP
Uplink Table
------------
Type State Priority In Use
---- ----- -------- ------
eth0 UP 0 Yes
Wifi-sta LOAD 6 No
3G/4G INIT 7 No
Internet failover :disable
Max allowed test packet loss:10
Secs between test packets :30
VPN failover timeout (secs) :180
ICMP pkt sent :0
ICMP pkt lost :0
Continuous pkt lost :0
VPN down time :0

Instant Access Point# show uplink config

Uplink preemption :enable
Uplink enforce :none
Ethernet uplink bond0 :DHCP
Internet failover :disable
Max allowed test packet loss:10
Secs between test packets :30
VPN failover timeout (secs) :180
```

The Intrusion Detection System (IDS) is a feature that monitors the network for the presence of unauthorized W-IAPs and clients. It also logs information about the unauthorized W-IAPs and clients, and generates reports based on the logged information.

The IDS feature in the Instant network enables you to detect rogue APs, interfering APs, and other devices that can potentially disrupt network operations.

This chapter describes the following procedures:

- Detecting and Classifying Rogue APs on page 296
- OS Fingerprinting on page 296
- Configuring Wireless Intrusion Protection and Detection Levels on page 297
- Configuring IDS Using CLI on page 301

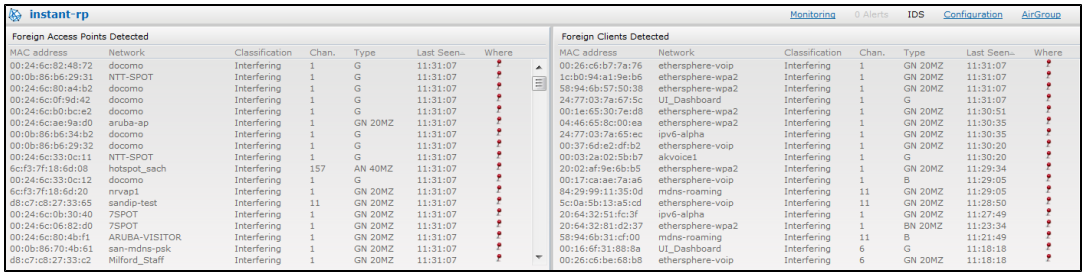
Detecting and Classifying Rogue APs

A rogue AP is an unauthorized AP plugged into the wired side of the network.

An interfering AP is an AP seen in the RF environment but it is not connected to the wired network. While the interfering AP can potentially cause RF interference, it is not considered a direct security threat, because it is not connected to the wired network. However, an interfering AP may be reclassified as a rogue AP.

To detect the rogue APs, click the **IDS** link in the Instant main window. The built-in IDS scans for access points that are not controlled by the Virtual Controller. These are listed and classified as either Interfering or Rogue, depending on whether they are on a foreign network or your network.

Figure 110 *Intrusion Detection*


instant-rp
Monitoring
Alerts
IDS
Configuration
AirGroup
Foreign Access Points Detected
MAC address
Network
Classification
Chan.
Type
Last Seen
Where
00:24:6c:82:48:72 docomo Interfering 1 G 11:31:07
00:0b:86:b6:29:31 NTT-SPOT Interfering 1 G 11:31:07
00:24:6c:80:a4:b2 docomo Interfering 1 G 11:31:07
00:24:6c:0f:9d:42 docomo Interfering 1 G 11:31:07
00:24:6c:b0:bc:e2 docomo Interfering 1 G 11:31:07
00:24:6c:ae:9a:d0 aruba-ap Interfering 1 GN 20MZ 11:31:07
00:0b:86:b6:34:b2 docomo Interfering 1 G 11:31:07
00:0b:86:b6:29:32 docomo Interfering 1 G 11:31:07
00:24:6c:33:0c:11 NTT-SPOT Interfering 1 G 11:31:07
6c:f3:7f:18:6d:08 hotspot_sach Interfering 157 AN 40MZ 11:31:07
00:24:6c:33:0c:12 docomo Interfering 1 G 11:31:07
6c:f3:7f:18:6d:20 nrvap1 Interfering 1 GN 20MZ 11:31:07
d8:c7:c8:27:33:65 sandip-test Interfering 11 GN 20MZ 11:31:07
00:24:6c:0b:30:40 7SPOT Interfering 1 GN 20MZ 11:31:07
00:24:6c:06:82:d0 7SPOT Interfering 1 GN 20MZ 11:31:07
00:24:6c:80:4b:f1 ARUBA-VISITOR Interfering 1 GN 20MZ 11:31:07
00:0b:86:70:4b:61 san-mdns-psk Interfering 1 GN 20MZ 11:31:07
d8:c7:c8:27:33:c2 Milford_Staff Interfering 1 GN 20MZ 11:31:07
Foreign Clients Detected
MAC address
Network
Classification
Chan.
Type
Last Seen
Where
00:26:c6:b7:7a:76 ethersphere-voip Interfering 1 GN 20MZ 11:31:07
1c:b0:94:a1:9e:b6 ethersphere-wpa2 Interfering 1 GN 20MZ 11:31:07
58:94:6b:57:50:38 ethersphere-wpa2 Interfering 1 GN 20MZ 11:31:07
24:77:03:7a:67:5c UI_Dashboard Interfering 1 G 11:31:07
00:1e:65:30:7e:d8 ethersphere-wpa2 Interfering 1 GN 20MZ 11:30:51
04:46:65:8c:00:ea ethersphere-wpa2 Interfering 1 GN 20MZ 11:30:35
24:77:03:7a:65:ec ipv6-alpha Interfering 1 GN 20MZ 11:30:35
00:37:6d:e2:df:b2 ethersphere-voip Interfering 1 GN 20MZ 11:30:20
00:03:2a:02:5b:b7 akvoice1 Interfering 1 G 11:30:20
20:02:af:9e:6b:b5 ethersphere-wpa2 Interfering 1 GN 20MZ 11:29:34
00:17:ca:ae:7a:a6 ethersphere-voip Interfering 1 B 11:29:05
84:29:99:11:35:0d mdns-roaming Interfering 11 GN 20MZ 11:29:05
5c:0a:5b:13:a5:cd ethersphere-voip Interfering 11 GN 20MZ 11:28:50
20:64:32:51:fc:3f ipv6-alpha Interfering 1 GN 20MZ 11:27:49
20:64:32:81:d2:37 ethersphere-wpa2 Interfering 1 BN 20MZ 11:23:34
58:94:6b:31:cf:00 mdns-roaming Interfering 11 B 11:21:49
00:16:6f:31:88:8a UI_Dashboard Interfering 6 G 11:18:18
00:26:c6:be:68:b8 ethersphere-voip Interfering 6 GN 20MZ 11:18:18

OS Fingerprinting

The OS Fingerprinting feature gathers information about the client that is connected to the Instant network to find the operating system that the client is running on. The following is a list of advantages of this feature:

- Identifying rogue clients– Helps to identify clients that are running on forbidden operating systems.
- Identifying outdated operating systems– Helps to locate outdated and unexpected OS in the company network.
- Locating and patching vulnerable operating systems– Assists in locating and patching specific operating system versions on the network that have known vulnerabilities, thereby securing the company network.

OS Fingerprinting is enabled in the Instant network by default. The following operating systems are identified by Instant:

- Windows 7

- Windows Vista
- Windows Server
- Windows XP
- Windows ME
- OS-X
- iPhone
- iOS
- Android
- Blackberry
- Linux

Configuring Wireless Intrusion Protection and Detection Levels

WIP offers a wide selection of intrusion detection and protection features to protect the network against wireless threats.

Like most other security-related features of the Instant network, the WIP can be configured on the W-IAP.

You can configure the following options:

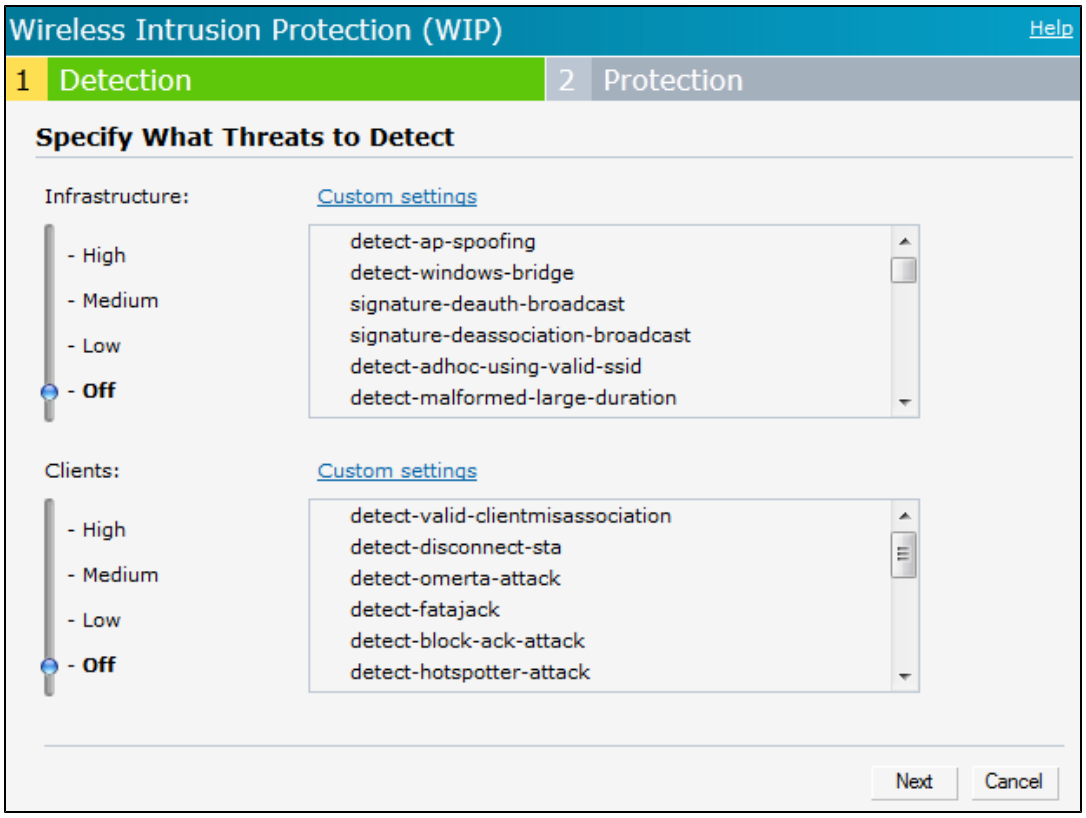
- **Infrastructure Detection Policies**– Specifies the policy for detecting wireless attacks on access points.
- **Client Detection Policies**– Specifies the policy for detecting wireless attacks on clients.
- **Infrastructure Protection Policies**– Specifies the policy for protecting access points from wireless attacks.
- **Client Protection Policies**– Specifies the policy for protecting clients from wireless attacks.
- **Containment Methods**– Prevents unauthorized stations from connecting to your Instant network.

Each of these options contains several default levels that enable different sets of policies. An administrator can customize enable or disable these options accordingly.

The detection levels can be configured using the **IDS** window. To view the IDS window, click **More** > **IDS** link at the top right corner of the Instant main window. The following levels of detection can be configured in the WIP Detection page:

- **Off**
- **Low**
- **Medium**
- **High**

Figure 111 *Wireless Intrusion Detection*



The following table describes the detection policies enabled in the Infrastructure Detection **Custom settings** field.

Table 55: *Infrastructure Detection Policies*

Detection Level	Detection Policy
Off	Rogue Classification
Low	• Detect AP Spoofing • Detect Windows Bridge • IDS Signature– Deauthentication Broadcast • IDS Signature– Deassociation Broadcast
Medium	• Detect Adhoc networks using VALID SSID– Valid SSID list is auto-configured based on Instant AP configuration • Detect Malformed Frame– Large Duration
High	• Detect AP Impersonation • Detect Adhoc Networks • Detect Valid SSID Misuse • Detect Wireless Bridge • Detect 802.11 40MHz intolerance settings • Detect Active 802.11n Greenfield Mode • Detect AP Flood Attack • Detect Client Flood Attack • Detect Bad WEP • Detect CTS Rate Anomaly • Detect RTS Rate Anomaly • Detect Invalid Address Combination

Table 55: *Infrastructure Detection Policies*

Detection Level	Detection Policy
	• Detect Malformed Frame– HT IE • Detect Malformed Frame– Association Request • Detect Malformed Frame– Auth • Detect Overflow IE • Detect Overflow EAPOL Key • Detect Beacon Wrong Channel • Detect devices with invalid MAC OUI

The following table describes the detection policies enabled in the Client Detection **Custom settings** field.

Table 56: *Client Detection Policies*

Detection Level	Detection Policy
Off	All detection policies are disabled.
Low	• Detect Valid Station Misassociation
Medium	• Detect Disconnect Station Attack • Detect Omerta Attack • Detect FATA-Jack Attack • Detect Block ACK DOS • Detect Hotspotter Attack • Detect unencrypted Valid Client • Detect Power Save DOS Attack
High	• Detect EAP Rate Anomaly • Detect Rate Anomaly • Detect Chop Chop Attack • Detect TKIP Replay Attack • IDS Signature– Air Jack • IDS Signature– ASLEAP

The following levels of detection can be configured in the WIP Protection page:

- **Off**
- **Low**
- **High**

Figure 112 *Wireless Intrusion Protection*

The following table describes the protection policies that are enabled in the Infrastructure Protection **Custom settings** field.

Table 57: *Infrastructure Protection Policies*

Protection Level	Protection Policy
Off	All protection policies are disabled
Low	• Protect SSID - Valid SSID list should be auto derived from Instant configuration • Rogue Containment
High	• Protect from Adhoc Networks • Protect AP Impersonation

The following table describes the detection policies that are enabled in the Client Protection **Custom settings** field.

Table 58: *Client Protection Policies*

Protection Level	Protection Policy
Off	All protection policies are disabled
Low	Protect Valid Station
High	Protect Windows Bridge

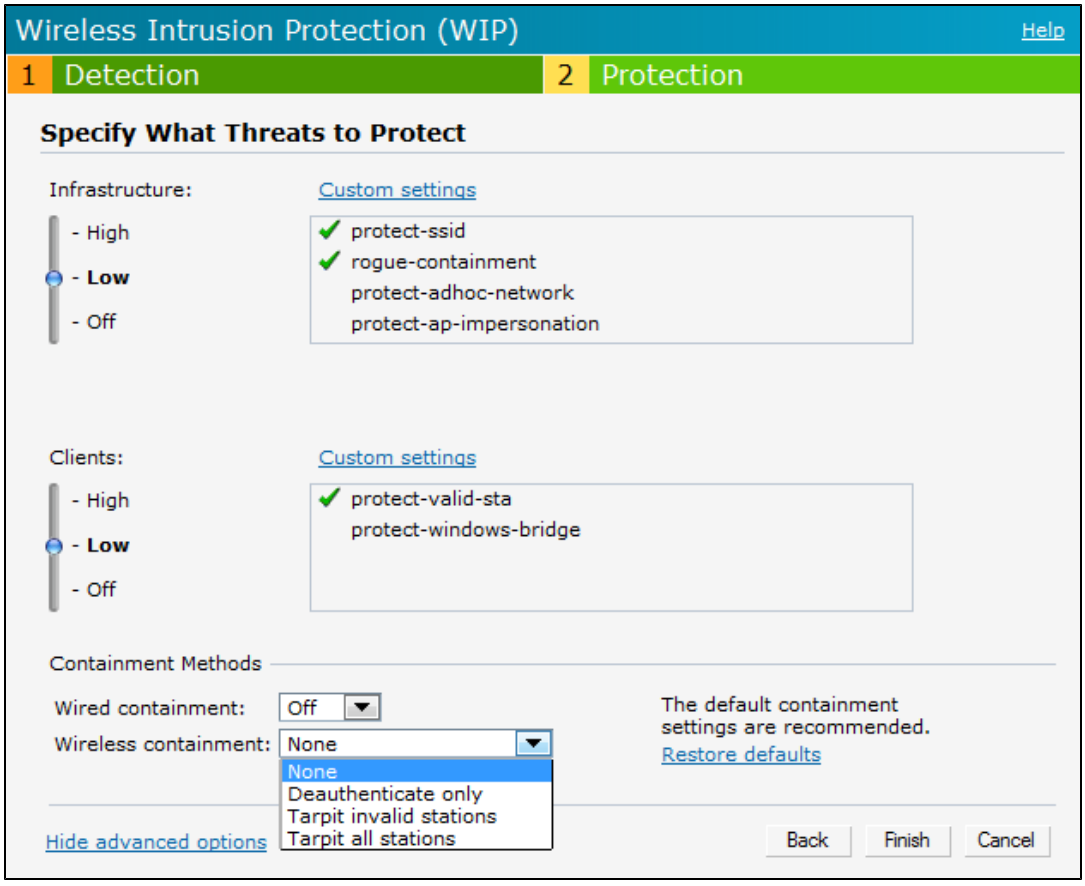
Containment Methods

You can enable wired and wireless containments to prevent unauthorized stations from connecting to your Instant network.

Instant supports the following types of containment mechanisms:

- Wired containment– When enabled, W-IAPs generate ARP packets on the wired network to contain wireless attacks.
- Wireless containment– When enabled, the system attempts to disconnect all clients that are connected or attempting to connect to the identified Access Point.
  - None– Disables all the containment mechanisms.
  - Deauthenticate only– With deauthentication containment, the Access Point or client is contained by disrupting the client association on the wireless interface.
  - Tarpit containment– With Tarpit containment, the Access Point is contained by luring clients that are attempting to associate with it to a tarpit. The tarpit can be on the same channel or a different channel as the Access Point being contained.

Figure 113 *Containment Methods*



Configuring IDS Using CLI

To configure IDS using CLI:

```
(Instant AP)(config)# ids
(Instant AP)(IDS)# infrastructure-detection-level <type>
(Instant AP)(IDS)# client-detection-level <type>
(Instant AP)(IDS)# infrastructure-protection-level <type>
(Instant AP)(IDS)# client-protection-level <type>
```

```
(Instant AP)(IDS)# wireless-containment <type>
(Instant AP)(IDS)# wired-containment
(Instant AP)(IDS)# detect-ap-spoofing
(Instant AP)(IDS)# detect-windows-bridge
(Instant AP)(IDS)# signature-deauth-broadcast
(Instant AP)(IDS)# signature-deassociation-broadcast
(Instant AP)(IDS)# detect-adhoc-using-valid-ssid
(Instant AP)(IDS)# detect-malformed-large-duration
(Instant AP)(IDS)# detect-ap-impersonation
(Instant AP)(IDS)# detect-adhoc-network
(Instant AP)(IDS)# detect-valid-ssid-misuse
(Instant AP)(IDS)# detect-wireless-bridge
(Instant AP)(IDS)# detect-ht-40mhz-intolerance
(Instant AP)(IDS)# detect-ht-greenfield
(Instant AP)(IDS)# detect-ap-flood
(Instant AP)(IDS)# detect-client-flood
(Instant AP)(IDS)# detect-bad-wep
(Instant AP)(IDS)# detect-cts-rate-anomaly
(Instant AP)(IDS)# detect-rts-rate-anomaly
(Instant AP)(IDS)# detect-invalid-addresscombination
(Instant AP)(IDS)# detect-malformed-htie
(Instant AP)(IDS)# detect-malformed-assoc-req
(Instant AP)(IDS)# detect-malformed-frame-auth
(Instant AP)(IDS)# detect-overflow-ie
(Instant AP)(IDS)# detect-overflow-eapol-key
(Instant AP)(IDS)# detect-beacon-wrong-channel
(Instant AP)(IDS)# detect-invalid-mac-oui
(Instant AP)(IDS)# detect-valid-clientmisassociation
(Instant AP)(IDS)# detect-disconnect-sta
(Instant AP)(IDS)# detect-omerta-attack
(Instant AP)(IDS)# detect-fatajack
(Instant AP)(IDS)# detect-block-ack-attack
(Instant AP)(IDS)# detect-hotspotter-attack
(Instant AP)(IDS)# detect-unencrypted-valid
(Instant AP)(IDS)# detect-power-save-dos-attack
(Instant AP)(IDS)# detect-eap-rate-anomaly
(Instant AP)(IDS)# detect-rate-anomalies
(Instant AP)(IDS)# detect-chopchop-attack
(Instant AP)(IDS)# detect-tkip-replay-attack
(Instant AP)(IDS)# signature-airjack
(Instant AP)(IDS)# signature-asleap
(Instant AP)(IDS)# protect-ssid
(Instant AP)(IDS)# rogue-containment
(Instant AP)(IDS)# protect-adhoc-network
(Instant AP)(IDS)# protect-ap-impersonation
(Instant AP)(IDS)# protect-valid-sta
(Instant AP)(IDS)# protect-windows-bridge
(Instant AP)(IDS)# end
(Instant AP)# commit apply
```

This chapter provides the following information:

- Mesh Network Overview on page 303
- Setting up Instant Mesh Network on page 304
- Configuring Wired Bridging on Ethernet 0 for Mesh Point on page 304

Mesh Network Overview

The Dell Instant secure enterprise mesh solution is an effective way to expand network coverage for outdoor and indoor enterprise environments without any wires. As traffic traverses across mesh W-IAPs, the mesh network automatically reconfigures around broken or blocked paths. This self-healing feature provides increased reliability and redundancy and allows the network to continue operation even when a W-IAP stops functioning or if a connection fails.

Mesh W-IAPs

Mesh network requires at least one valid uplink (wired or 3G) connection. Any provisioned W-IAP that has a valid uplink (wired or 3G) functions as a mesh portal, and the W-IAP without an Ethernet link functions as a mesh point. The mesh portal can also act as a Virtual Controller. Mesh portals and mesh points are also known as mesh nodes, a generic term used to describe W-IAPs configured for mesh.

If two W-IAPs have valid uplink connections, there is redundancy in the mesh network, and most mesh points try to mesh directly with one of the two portals. However, depending on the actual deployment and RF environment, some mesh points may mesh through other intermediate mesh points.

In a Instant mesh network, the maximum hop count is two nodes (point >point >portal) and the maximum number of mesh points per mesh portal is eight.

Mesh W-IAPs detect the environment when they boot up, locate and associate with their nearest neighbor, to determine the best path to the mesh portal.

Instant mesh functionality is supported only on dual radio W-IAPs only. On dual-radio W-IAPs, the 5 GHz radio is always used for both mesh-backhaul and client traffic, while the 2.4 GHz radio is always used for client traffic.

Mesh service is automatically enabled on 802.11a band for dual-radio W-IAP only, and this is not configurable.

For W-IAP-RW variants, the mesh network must be provisioned for the first time by plugging into the wired network. After that, mesh works on W-IAP-RWs like any other regulatory domain.

Mesh Portals

A mesh portal (MPP) is a gateway between the wireless mesh network and the enterprise wired LAN. The mesh roles are automatically assigned based on the W-IAP configuration. A mesh network could have multiple mesh portals to support redundant mesh paths (mesh links between neighboring mesh points that establish the best path to the mesh portal) from the wireless mesh network to the wired LAN.

The mesh portal broadcasts a mesh services set identifier (MSSID/ mesh cluster name) to advertise the mesh network service to other mesh points in that Instant network. This is not configurable and is transparent to the user. The mesh points authenticate to the mesh portal and establish a link that is secured using Advanced Encryption Standard (AES) encryption.

The mesh portal reboots after 5 minutes when it loses its uplink connectivity to a wired network.

Mesh Points

The mesh point establishes an all-wireless path to the mesh portal. The mesh point provides traditional WLAN services such as client connectivity, intrusion detection system (IDS) capabilities, user role association, and Quality of Service (QoS) for LAN-to-mesh communication to clients and performs mesh backhaul/network connectivity.

Mesh point also supports LAN bridging. You can connect any wired device to the downlink port of the mesh point. In the case of single Ethernet port platforms such as AP-93 and AP-105, you can convert the Eth0 uplink port to a downlink port by enabling **Eth0 Bridging**. For additional information, see Configuring Wired Bridging on Ethernet 0 for Mesh Point on page 304.

Setting up Instant Mesh Network

Starting from Instant 6.4.0.2-4.1 release, mesh functionality is disabled by default, because of which over-the-air provisioning of mesh W-IAPs is not supported.

To provision W-IAPs as mesh W-IAPs:

1. Connect the W-IAPs to a wired switch.
2. Ensure that the Virtual Controller key is synchronized and the country code is configured.
3. Ensure that a valid SSID is configured on the W-IAP.
4. If the IAP has a factory default SSID (instant SSID), delete the SSID.
5. If an extended SSID is enabled on the virtual controller, disable it and reboot the W-IAP cluster.
6. Disconnect the W-IAPs that you want to deploy as mesh points from the switch and place the W-IAPs at a remote location. The W-IAPs power on without any wired uplink connection and function as mesh points and the W-IAPs with valid uplink connections function as the mesh portal.

Instant does not support the topology in which the W-IAPs are connected to the downlink ethernet port of a mesh point.

Configuring Wired Bridging on Ethernet 0 for Mesh Point

Instant supports wired bridging on the Ethernet 0 port of a W-IAP. If W-IAP is configured to function as a mesh point, you can configure wired bridging.

Enabling wired bridging on this port of a W-IAP makes the port available as a downlink wired bridge and allows client access through the port.

When using 3G uplink, the wired port will be used as downlink.

You can configure support for wired bridging on the Ethernet 0 port of a W-IAP using the Instant UI or CLI.

In the Instant UI

To configure Ethernet bridging:

1. In the **Access Points** tab, click the W-IAP to modify. The **edit** link is displayed.
2. Click the **edit** link. The **edit** window for modifying W-IAP details is displayed.
3. Click the **Uplink** tab.
4. Select **Enable** from the **Eth0 Bridging** drop-down list.
5. Click **OK**.
6. Reboot the W-IAP.

In the CLI

To configure Ethernet bridging:

```
Instant Access Point# enet0-bridging
```

Make the necessary changes to the wired-profile when eth0 is used as the downlink port. For more information, see the Configuring a Wired Profile on page 112

This chapter provides the following information:

- Layer-3 Mobility Overview on page 306
- Configuring L3-Mobility on page 307

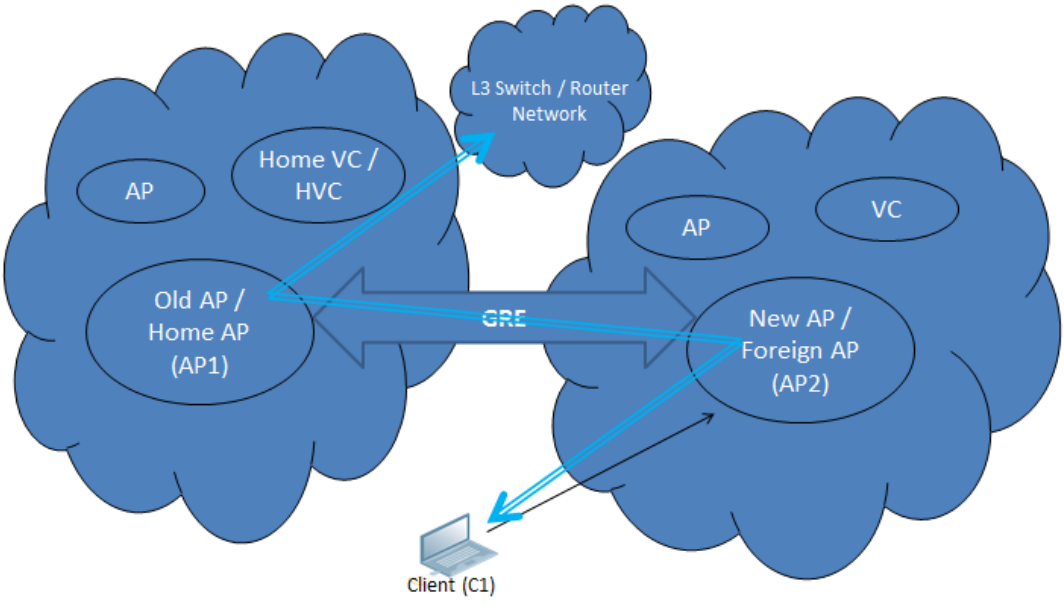
Layer-3 Mobility Overview

W-IAPs form a single Instant network when they are in the same Layer-2 (L2) domain. As the number of clients increase, multiple subnets are required to avoid broadcast overhead. In such a scenario, a client must be allowed to roam away from the Instant network to which it first connected (home network) to another network supporting the same WLAN access parameters (foreign network) and continue its existing sessions.

Layer-3 (L3) mobility allows a client to roam without losing its IP address and sessions. If WLAN access parameters are the same across these networks, clients connected to W-IAPs in a given Instant network can roam to APs in a foreign Instant network and continue their existing sessions. Clients roaming across these networks are able to continue using their IP addresses after roaming. You can configure a list of Virtual Controller IP addresses across which L3 mobility is supported.

The Dell Networking W-Series Instant Layer-3 mobility solution defines a Mobility Domain as a set of Instant networks, with the same WLAN access parameters, across which client roaming is supported. The Instant network to which the client first connects is called its home network. When the client roams to a foreign network, an AP in the home network (home AP) anchors all traffic to or from this client. The AP to which the client is connected in the foreign network (foreign AP) tunnels all client traffic to or from the home AP through a GRE tunnel.

Figure 114 *Routing of traffic when the client is away from its home network*



When a client first connects to an Instant network, a message is sent to all configured Virtual Controller IP addresses to see if this is an L3 roamed client. On receiving an acknowledgement from any of the configured Virtual Controller IP addresses, the client is identified as an L3 roamed client. If the AP has no GRE tunnel to this home network, a new tunnel is formed to an AP (home AP) from the client's home network.

Each foreign AP has only one home AP per Instant network to avoid duplication of broadcast traffic. Separate GRE tunnels are created for each foreign AP / home AP pair. If a peer AP is a foreign AP for one client and a home AP for another, two separate GRE tunnels are used to handle L3 roaming traffic between these APs.

If client subnet discovery fails on association due to some reason, the foreign AP identifies its subnet when it sends out the first L3 packet. If the subnet is not a local subnet and belongs to another Instant network, the client is treated as an L3 roamed client and all its traffic is forwarded to the home network through a GRE tunnel.

Configuring L3-Mobility

To configure a mobility domain, you have to specify the list of all Instant networks that form the mobility domain. To allow clients to roam seamlessly among all the APs, specify the Virtual Controller IP for each foreign subnet. You may include the local Instant or Virtual Controller IP address, so that the same configuration can be used across all Instant networks in the mobility domain.

It is recommended that you configure all client subnets in the mobility domain. When client subnets are configured:

- If a client is from a local subnet, it is identified as a local client. When a local client starts using the IP address, the L3 roaming is terminated.
- If the client is from a foreign subnet, it is identified as a foreign client. When a foreign client starts using the IP address, the L3 roaming is set up.

Home Agent Load Balancing

Home Agent Load Balancing is required in large networks where multiple tunnels might terminate on a single border or lobby AP and overload it. When load balancing is enabled, the Virtual Controller assigns the home AP for roamed clients by using a *round robin* policy. With this policy, the load for the APs acting as Home Agents for roamed clients is uniformly distributed across the W-IAP cluster.

Configuring a Mobility Domain for Instant

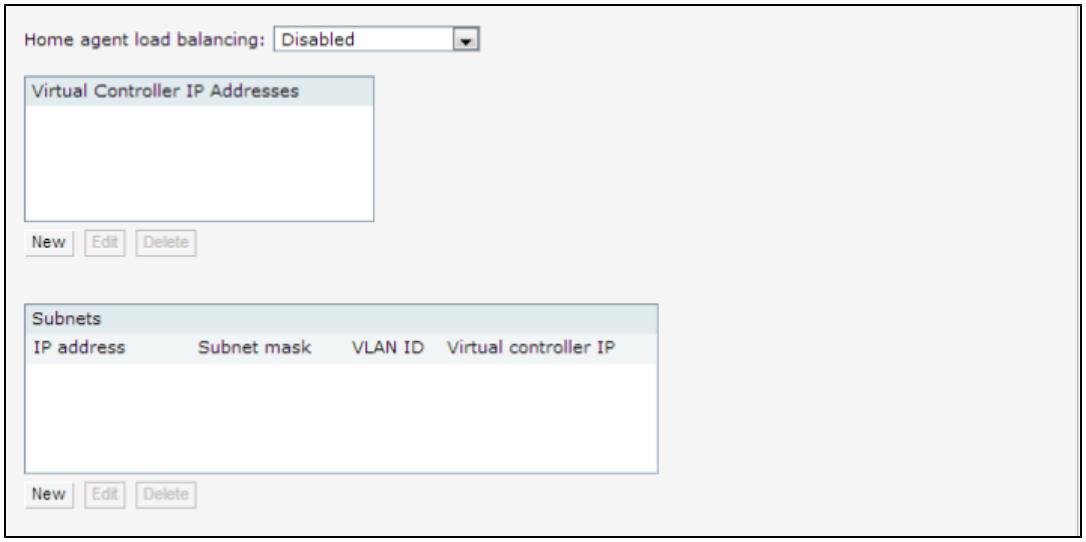
You can configure L3 mobility domain by using the Instant UI or CLI.

In the Instant UI

To configure a mobility domain, perform the following steps:

1. Click the **System** link at top right corner of the Instant main window. The **System** window is displayed.
2. Click the **Show advanced options** link. The advanced options are displayed.
3. Click **L3 Mobility**. The L3 Mobility window is displayed.

Figure 115 *L3 Mobility Window*



4. Select **Enabled** from the **Home agent load balancing** drop-down list. By default, home agent load balancing is disabled.
5. Click **New** in the **Virtual Controller IP Addresses** section, add the IP address of a Virtual Controller that is part of the mobility domain, and click **OK**.
6. Repeat Step 2 to add the IP addresses of all Virtual Controllers that form the L3 mobility domain.
7. Click **New** in the **Subnets** section and specify the following:
   a. Enter the client subnet in the **IP address** text box.
   b. Enter the mask in the **Subnet mask** text box.
   c. Enter the VLAN ID in the home network in the **VLAN ID** text box.
   d. Enter the home VC IP address for this subnet in the **Virtual Controller IP** text box.
8. Click **OK**.

In the CLI

To configure a mobility domain:

```
(Instant AP)(config)# l3-mobility
(Instant AP)(L3-mobility)# home-agent-load-balancing
(Instant AP)(L3-mobility)# virtual-controller <IP-address>
(Instant AP)(L3-mobility)# subnet <IP-address> <subnet-mask> <VLAN-ID> <virtual-controller-IP-address>
(Instant AP)(L3-mobility)# end
(Instant AP)# commit apply
```

This chapter provides the following information:

- Understanding Spectrum Data on page 309
- Configuring Spectrum Monitors and Hybrid W-IAPs on page 314

Understanding Spectrum Data

Wireless networks operate in environments with electrical and radio frequency devices that can interfere with network communications. Microwave ovens, cordless phones, and even adjacent Wi-Fi networks are all potential sources of continuous or intermittent interference. The spectrum monitor software modules on W-IAPs that support this feature are able to examine the radio frequency (RF) environment in which the Wi-Fi network is operating, identify interference and classify its sources. An analysis of the results can then be used to quickly isolate issues with packet transmission, channel quality, and traffic congestion caused by contention with other devices operating in the same band or channel.

Spectrum monitors (SMs) are W-IAP radios that gather spectrum data but do not service clients. Each SM scans and analyzes the spectrum band used by the SM's radio (2.4 GHz or 5 GHz). An AP radio in hybrid AP mode continues to serve clients as an access point while it analyzes spectrum analysis data for the channel the radio uses to serve clients. You can record data for both types of spectrum monitor devices. However, the recorded spectrum is not reported to the Virtual Controller. A spectrum alert is sent to the VC when a non Wi-Fi interference device is detected.

The spectrum monitor is supported on W-IAP103, W-IAP104/105, W-IAP134/135, W-IAP114/115, and W-IAP224/225 radios.

The spectrum data is collected by each W-IAP spectrum monitor and hybrid AP. The spectrum data is not reported to the VC. The **Spectrum** link is visible in the UI (Access Point view) only if you have enabled the spectrum monitoring feature. You can view the following spectrum data in the UI:

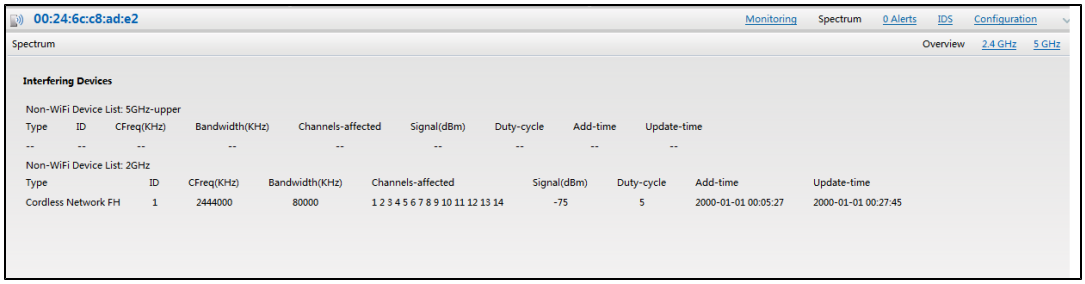
- Device List
- Non Wi-Fi Interferers
- Channel Metrics
- Channel Details
- Spectrum Alerts

Device List

The device list consists of a device summary table and channel information for active non Wi-Fi devices currently seen by a spectrum monitor or hybrid AP radio.

To view the device list, click **Spectrum** in the dashboard. The following figure shows an example of the device list details.

Figure 116 *Device List*


00:24:6c:c8:ad:e2
Monitoring
Spectrum
0 Alerts
IDS
Configuration
Spectrum
Overview
2.4 GHz
5 GHz
Interfering Devices
Non-WiFi Device List: 5GHz-upper
Type ID CFreq(KHz) Bandwidth(KHz) Channels-affected Signal(dBm) Duty-cycle Add-time Update-time
-- -- -- -- -- -- -- --
Non-WiFi Device List: 2GHz
Type ID CFreq(KHz) Bandwidth(KHz) Channels-affected Signal(dBm) Duty-cycle Add-time Update-time
Cordless Network FH 1 2444000 80000 1 2 3 4 5 6 7 8 9 10 11 12 13 14 -75 5 2000-01-01 00:05:27 2000-01-01 00:27:45

Device Summary and Channel Information shows the details of the information that is displayed:

Table 59: *Device Summary and Channel Information*

Column	Description
Type	Device type. This parameter can be any of the following: • audio FF (fixed frequency) • bluetooth • cordless base FH (frequency hopper) • cordless phone FF (fixed frequency) • cordless network FH (frequency hopper) • generic FF (fixed frequency) • generic FH (frequency hopper) • generic interferer • microwave • microwave inverter • video • xbox **NOTE:** For additional details about non Wi-Fi device types shown in this table, see Non Wi-Fi Interferer Types.
ID	ID number assigned to the device by the spectrum monitor or hybrid AP radio. Spectrum monitors and hybrid APs assign a unique spectrum ID per device type.
Cfreq	Center frequency of the signal sent from the device.
Bandwidth	Channel bandwidth used by the device.
Channels-affected	Radio channels affected by the wireless device.
Signal-strength	Strength of the signal sent from the device, in dBm.
Duty-cycle	Device duty cycle. This value represents the percent of time the device broadcasts a signal.
Add-time	Time at which the device was first detected.
Update-time	Time at which the device's status was updated.

Non Wi-Fi Interferers

The following table describes each type of non Wi-Fi interferer detected by the spectrum monitor feature.

Table 60: *Non Wi-Fi Interferer Types*

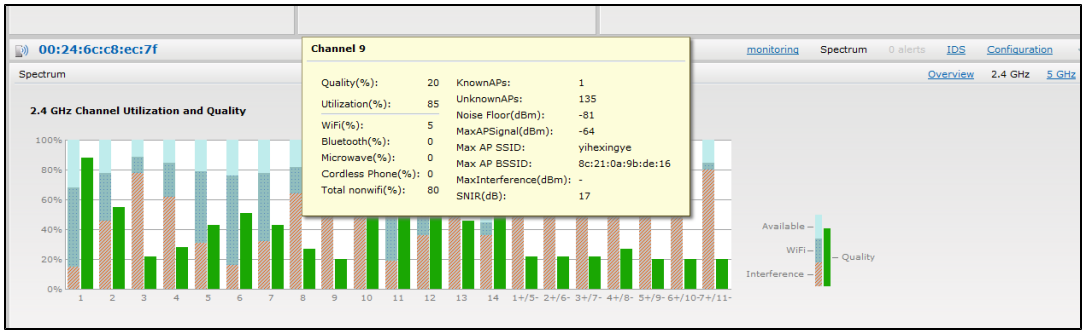
Non Wi-Fi Interferer	Description
Bluetooth	Any device that uses the Bluetooth protocol to communicate in the 2.4 GHz band is classified as a *Bluetooth* device. Bluetooth uses a frequency hopping protocol.
Fixed Frequency (Audio)	Some audio devices such as wireless speakers and microphones also use fixed frequency to continuously transmit audio. These devices are classified as *Fixed Frequency (Audio)*.
Fixed Frequency (Cordless Phones)	Some cordless phones use a fixed frequency to transmit data (much like the fixed frequency video devices). These devices are classified as *Fixed Frequency (Cordless Phones)*.
Fixed Frequency (Video)	Video transmitters that continuously transmit video on a single frequency are classified as *Fixed Frequency (Video)*. These devices typically have close to a 100% duty cycle. These types of devices may be used for video surveillance, TV or other video distribution, and similar applications.
Fixed Frequency (Other)	All other fixed frequency devices that do not fall into one of the above categories are classified as *Fixed Frequency (Other)*). Note that the RF signatures of the fixed frequency audio, video and cordless phone devices are very similar and that some of these devices may be occasionally classified as *Fixed Frequency (Other)*.
Frequency Hopper (Cordless Base)	Frequency hopping cordless phone base units transmit periodic beacon-like frames at all times. When the handsets are not transmitting (i.e., no active phone calls), the cordless base is classified as *Frequency Hopper (Cordless Bas)*.
Frequency Hopper (Cordless Network)	When there is an active phone call and one or more handsets are part of the phone conversation, the device is classified as *Frequency Hopper (Cordless Network)*. Cordless phones may operate in 2.4 GHz or 5 GHz bands. Some phones use both 2.4 GHz and 5 GHz bands (for example, 5 GHz for Base-to-handset and 2.4 GHz for Handset-to-base). These phones may be classified as unique Frequency Hopper devices on both bands.
Frequency Hopper (Xbox)	The Microsoft Xbox device uses a frequency hopping protocol in the 2.4 GHz band. These devices are classified as *Frequency Hopper (Xbox)*.
Frequency Hopper (Other)	When the classifier detects a frequency hopper that does not fall into one of the above categories, it is classified as *Frequency Hopper (Other)*. Some examples include IEEE 802.11 FHSS devices, game consoles and cordless/hands-free devices that do not use one of the known cordless phone protocols.

Non Wi-Fi Interferer	Description
Microwave	Common residential microwave ovens with a single magnetron are classified as a *Microwave*. These types of microwave ovens may be used in cafeterias, break rooms, dormitories and similar environments. Some industrial, healthcare or manufacturing environments may also have other equipment that behave like a microwave and may also be classified as a Microwave device.
Microwave (Inverter)	Some newer-model microwave ovens have the inverter technology to control the power output and these microwave ovens may have a duty cycle close to 100%. These microwave ovens are classified as *Microwave (Inverter)*. Dual-magnetron industrial microwave ovens with higher duty cycle may also be classified as Microwave (Inverter). There may be other equipment that behaves like inverter microwaves in some industrial, healthcare or manufacturing environments. Those devices may also be classified as Microwave (Inverter).
Generic Interferer	Any non-frequency hopping device that does not fall into one of the other categories described in this table is classified as a *Generic Interferer*. For example a Microwave-like device that does not operate in the known operating frequencies used by the Microwave ovens may be classified as a Generic Interferer. Similarly wide-band interfering devices may be classified as Generic Interferers.

Channel Details

When you move your mouse over a channel, the channel details or the summary of the 5 GHz and 2.4 GHz channels as detected by a spectrum monitor are displayed. You can view the aggregate data for each channel seen by the spectrum monitor radio, including the maximum AP power, interference and the signal-to-noise-and-interference Ratio (SNIR). SNIR is the ratio of signal strength to the combined levels of interference and noise on that channel. Spectrum monitors display spectrum data seen on all channels in the selected band, and hybrid APs display data from the one channel they are monitoring.

Figure 117 *Channel Details*



Channel Details Information shows the information that you can view in the channel details graph.

Table 61: *Channel Details Information*

Column	Description
Channel	An 802.11a or 802.11g radio channel.
Quality(%)	Current relative quality of the channel.
Utilization(%)	The percentage of the channel being used.

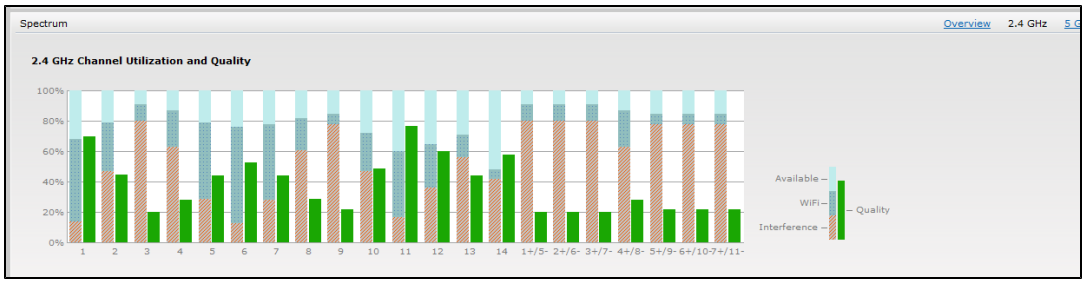
Column	Description
Wi-Fi (%)	The percentage of the channel currently being used by Wi-Fi devices.
Type	Device type.
Total nonwifi (%)	The percentage of the channel currently being used by non Wi-Fi devices.
Known APs	Number of valid APs identified on the radio channel.
UnKnown APs	Number of invalid or rogue APs identified on the radio channel.
Channel Util (%)	Percentage of the channel currently in use.
Max AP Signal (dBm)	Signal strength of the AP that has the maximum signal strength on a channel.
Max Interference (dBm)	Signal strength of the non Wi-Fi device that has the highest signal strength.
SNIR (db)	The ratio of signal strength to the combined levels of interference and noise on that channel. This value is calculated by determining the maximum noise-floor and interference-signal levels, and then calculating how strong the desired signal is above this maximum.

Channel Metrics

The channel metrics graph displays channel quality, availability and utilization metrics as seen by a spectrum monitor or hybrid AP. You can view the channel utilization data for the percentage of each channel that is currently being used by Wi-Fi devices, and the percentage of each channel being used by non Wi-Fi devices and 802.11 adjacent channel interference (ACI). This chart shows the channel availability, the percentage of each channel that is available for use, or the current relative quality of selected channels in the 2.4 GHz or 5 GHz radio bands. While spectrum monitors can display data for all channels in their selected band, hybrid APs display data for their one monitored channel only.

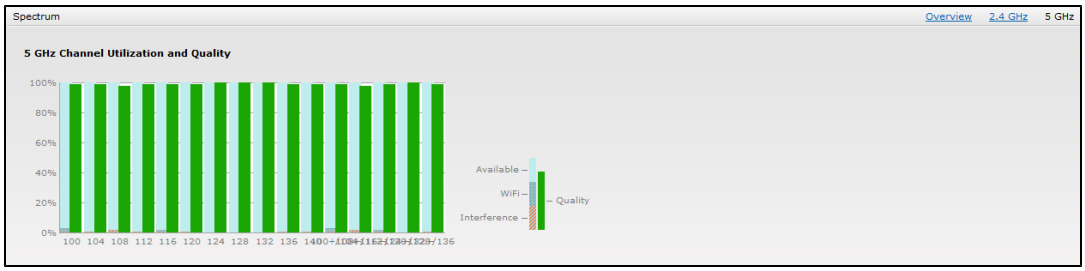
To view this graph, click **2.4 GHz** in the **Spectrum** section of the dashboard.

Figure 118 *Channel Metrics for the 2.4 GHz Radio Channel*



To view this graph, click **5 GHz** in the **Spectrum** section of the dashboard.

Figure 119 *Channel Metrics for the 5 GHz Radio Channel*



Channel Metrics shows the information displayed in the channel metrics graph.

Table 62: *Channel Metrics*

Column	Description
Channel	A 2.4 GHz or 5 GHz radio channel.
Quality(%)	Current relative quality of selected channels in the 2.4 GHz or 5 GHz radio bands, as determined by the percentage of packet retries, the current noise floor, and the duty cycle for non Wi-Fi devices on that channel.
Availability(%)	The percentage of the channel currently available for use.
Utilization(%)	The percentage of the channel being used.
WiFi Util(%)	The percentage of the channel currently being used by Wi-Fi devices.
Interference Util(%)	The percentage of the channel currently being used by non Wi-Fi interference + Wi-Fi ACI (Adjacent Channel Interference)

Spectrum Alerts

When a new non Wi-Fi device is found, an alert is reported to the Virtual Controller. The spectrum alert messages include the device ID, device type, IP address of the spectrum monitor or hybrid AP, and the timestamp. Virtual Controller reports the detailed device information to AMP.

Configuring Spectrum Monitors and Hybrid W-IAPs

A W-IAP can be provisioned to function as a spectrum monitor or as a hybrid W-IAP. The radios on groups of APs can be converted to dedicated spectrum monitors or hybrid APs via the AP group's 802.11a and 802.11g radio profiles.

Converting a W-IAP to a Hybrid W-IAP

You can convert all W-IAPs in an Instant network into hybrid W-IAPs by selecting the **Background spectrum monitoring** option in the 802.11a and 802.11g radio profiles of a W-IAP. APs in Access mode continue to provide normal access service to clients, while providing the additional function of monitoring RF interference. If any W-IAP in the Instant network does not support the spectrum monitoring feature, that AP continues to function as a standard W-IAP, rather than a hybrid W-IAP. By default, the background spectrum monitoring option is disabled. In the hybrid mode, spectrum monitoring is performed only on the home channel.

You can convert W-IAPs in a Instant network to hybrid mode using the Instant UI or CLI.

In the Instant UI

To convert a W-IAP to a hybrid W-IAP:

1. Click the **RF** link at the top right corner of the Instant UI.
2. Click **Show advanced options** to view the **Radio** tab.
3. To enable a spectrum monitor on the 802.11g radio band, in the 2.4 GHz radio profile, select **Enabled** from the **Background Spectrum Monitoring** drop-down list.
4. To enable a spectrum monitor on the 802.11a radio band, in the 5 GHz radio profile, select **Enabled** from the **Background Spectrum Monitoring** drop-down list.
5. Click **OK**.

In the CLI

To configure 2.4 GHz radio settings:

```
(Instant AP)(config)# rf dot11g-radio-profile
(Instant AP)(RF dot11 g Radio Profile)# spectrum-monitor
```

To configure 5 GHz radio settings:

```
(Instant AP)(config)# rf dot11a-radio-profile
(Instant AP)(RF dot11a Radio Profile)# spectrum-monitor
```

Converting a W-IAP to a Spectrum Monitor

In spectrum mode, spectrum monitoring is performed on entire bands. However, for the 5 GHz radio, spectrum monitoring is performed on only one of the three bands:

- 5 GHz - lower
- 5 GHz - middle
- 5 GHz - higher

By default, spectrum monitoring is performed on a higher band of the 5 GHz radio.

You can configure a W-IAP to function as a standalone spectrum monitor using the Instant UI or CLI.

In the Instant UI

To convert a W-IAP to a spectrum monitor:

1. In the **Access Points** tab, click the AP that you want to convert to a spectrum monitor. The **edit** link is displayed.
2. Click the **edit** link. The **Edit Access Point** window is displayed.
3. Click the **Radio** tab.
4. From the **Access Mode** drop-down list, select **Spectrum Monitor**.
5. Click **OK**.
6. Reboot the W-IAP for the changes to affect.
7. To enable spectrum monitoring for any other band for the 5 GHz radio:
   a. Click the **RF** link at the upper right corner of the Instant UI.
   b. Click **Show advanced options** to view the **Radio** tab.
   c. For the 5 GHz radio, specify the spectrum band you want that radio to monitor by selecting **Lower**, **Middle**, or **Higher** from the **Standalone spectrum band** drop-down list.
   d. Click **OK**.

In the CLI

To convert a W-IAP to a spectrum monitor:

```
(Instant AP)# wifi0-mode {<access>|<monitor>|<spectrum-monitor>}
(Instant AP)# wifi1-mode {<access>|<monitor>|<spectrum-monitor>}
```

To enable spectrum monitoring for any other band for the 5 GHz radio:

```
(Instant AP)(config)# rf dot11a-radio-profile
Instant Access Point (RF dot11a Radio Profile)# spectrum-band <type>
```

To view the radio configuration:

```
Instant Access Point# show radio config
2.4 GHz:
Legacy Mode:disable
Beacon Interval:100
802.11d/802.11h:disable
Interference Immunity Level:2
Channel Switch Announcement Count:0
Channel Reuse Type:disable
Channel Reuse Threshold:0
Background Spectrum Monitor:disable

5.0 GHz:
Legacy Mode:disable
Beacon Interval:100
802.11d/802.11h:disable
Interference Immunity Level:2
Channel Switch Announcement Count:0
Channel Reuse Type:disable
Channel Reuse Threshold:0
Background Spectrum Monitor:disable
Standalone Spectrum Band:5ghz-upper
```

This section provides information on the following procedures:

- Upgrading a W-IAP on page 317
- Backing up and Restoring W-IAP Configuration Data on page 319
- Converting a W-IAP to a Remote AP and Campus AP on page 320
- Resetting a Remote AP or Campus AP to a W-IAP on page 325
- Rebooting the W-IAP on page 325

Upgrading a W-IAP

While upgrading a W-IAP, you can use the image check feature to allow the W-IAP to find new software image versions available on a cloud-based image server hosted and maintained by Dell. The location of the image server is fixed and cannot be changed by the user. The image server is loaded with latest versions of Instant software.

Upgrading a W-IAP and Image Server

Instant supports mixed AP-class instant deployment with all APs as part of the same Virtual Controller cluster.

Image Management Using W-AirWave

If the multi-class W-IAP network is managed by W-AirWave, image upgrades can only be done through the W-AirWave UI. The W-IAP images for different classes must be uploaded on the AMP server. When new W-IAPs joining the network need to synchronize their software with the version running on the Virtual Controller, and if the new W-IAP belongs to a different class, the image file for the new W-IAP is provided by W-AirWave. If W-AirWave does not have the appropriate image file, the new AP will not be able to join the network.

The Virtual Controller communicates with the W-AirWave server if W-AirWave is configured. If W-AirWave is not configured on the W-IAP, the image is requested from the Image server.

Image Management Using Cloud Server

If the multi-class W-IAP network is not managed by W-AirWave, image upgrades can be done through the cloud-based image check feature. When a new W-IAP joining the network needs to synchronize its software version with the version on the Virtual Controller and if the new W-IAP belongs to a different class, the image file for the new W-IAP is provided by the cloud server.

Configuring HTTP Proxy on a W-IAP

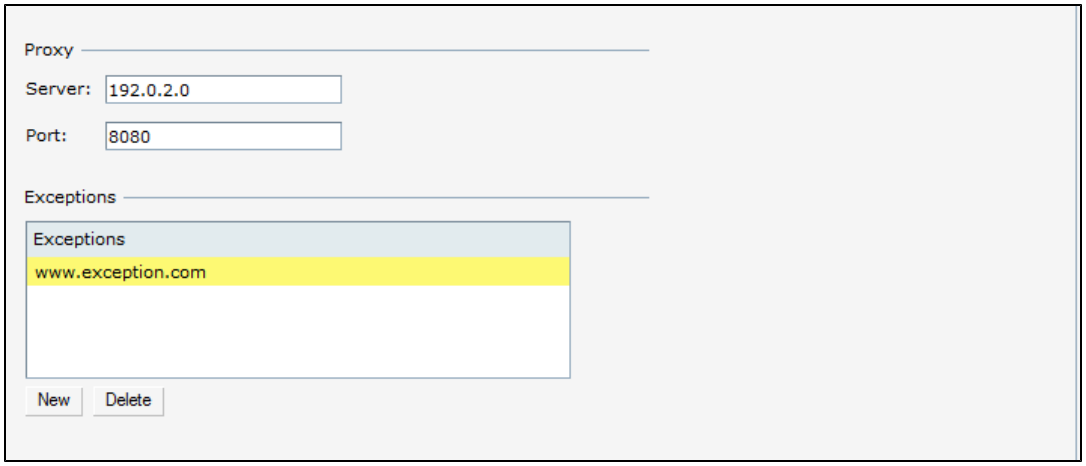
If your network requires a proxy server for internet access, you must first configure the HTTP proxy on the W-IAP to download the image from the cloud server. After you setup the HTTP proxy settings, the W-IAP connects to the Activate server, W-AirWave Management platform or OpenDNS server through a secure HTTP connection. You can also exempt certain applications from using the HTTP proxy (configured on a W-IAP) by providing their hostname or IP address under exceptions.

In the Instant UI

Perform these steps to configure the HTTP proxy settings:

1. Navigate to **System > Proxy**. The proxy configuration window is displayed.

Figure 120 *Proxy Configuration Window*



2. Enter the HTTP proxy server's IP address and the port number.
3. If you do not want the HTTP proxy to be applied for a particular host, click **New** to enter that IP address or domain name of that host under exceptions list.

In the CLI

```
(Instant AP)(config)# proxy server 192.0.2.1 8080
(Instant AP)(config)# proxy exception 192.0.2.2
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Upgrading a W-IAP Using Automatic Image Check

You can upgrade a W-IAP by using the automatic image check feature. The Automatic image checks are performed once after the AP boots up and every week thereafter.

If the image check locates a new version of the Instant software on the image server, the **New version available** link is displayed at the top right corner of the UI.

If W-AirWave is configured, the automatic image check is disabled.

To check for a new version on the image server in the cloud:

1. Go to **Maintenance**>**Automatic**>**Check for New Version**. After the image check is completed, one of the following messages is displayed:
   - No new version available – If there is no new version available.
   - Image server timed out – Connection or session between the image server and the W-IAP is timed out.
   - Image server failure – If the image server does not respond.
   - A new image version found – If a new image version is found.
2. If a new version is found, the **Upgrade Now** button becomes available and the version number is displayed.
3. Click **Upgrade Now**.

   The W-IAP downloads the image from the server, saves it to flash and reboots. Depending on the progress and success of the upgrade, one of the following messages is displayed:
   - Upgrading – While image upgrading is in progress.
   - Upgrade successful – When the upgrading is successful.
   - Upgrade failed – When the upgrading fails.

If the upgrade fails and an error message is displayed, retry upgrading the W-IAP.

Upgrading to a New Version Manually

If the automatic image check feature is disabled, you can use obtain an image file from a local file system or from a TFTP or HTTP URL. To manually check for a new firmware image version and obtain an image file:

1. Navigate to **Maintenance**>**Firmware**. The Firmware window is displayed.
2. Under **Manual** section, perform the following steps:

- Select the **Image file** option. This method is only available for single-class W-IAPs.

  The following examples describe the image file format for different W-IAP models:

  - For W-IAP134/135 – DellInstant_Cassiopeia_6.4.0.2-4.1.0.0_xxxx
  - For W-IAP108/109, W-IAP103, and W-IAP114/115– DellInstant_Pegasus_6.4.0.2-4.1.0.0_xxxx
  - For W-IAP155/155P – DellInstant_Aries_6.4.0.2-4.1.0.0_xxxx
  - For W-IAP220 Series and W-IAP270 Series – DellInstant_Centaurus_6.4.0.2-4.1.0.0_xxxx
  - For all other W-IAPs –DellInstant_Orion_6.4.0.2-4.1.0.0_xxxx
- Select the **Image URL** option. Select this option to obtain an image file from a TFTP, FTP, or HTTP URL.
  - HTTP - http://<IP-address>/<image-file>. For example, http://<IP-address>/DellInstant_Orion_6.4.0.2-4.1.0.0_xxxx
  - TFTP - tftp://<IP-address>/<image-file>. For example, tftp://<IP-address>/DellInstant_Orion_6.4.0.2-4.1.0.0_xxxx
  - FTP - ftp://<IP-address>/<image-file>. For example, ftp://<IP-address>/DellInstant_Orion_6.4.0.2-4.1.0.0_xxxx

3. Clear the **Reboot all APs after upgrade** checkbox if required. The **Reboot all APs after upgrade** checkbox is selected by default to allow the W-IAPs to reboot automatically after a successful upgrade. To reboot the W-IAP at a later time, clear the **Reboot all APs after upgrade** checkbox.
4. Click **Upgrade Now** to upgrade the W-IAP to the newer version.

Upgrading an Image Using CLI

To upgrade an image using a HTTP, TFTP, or FTP URL:

```
(Instant AP)# upgrade-image <ftp/tftp/http-URL>
```

To upgrade an image without rebooting the W-IAP:

```
(Instant AP)# upgrade-image2-no-reboot <ftp/tftp/http-URL>
```

To view the upgrade information:

```
(Instant AP)# show upgrade info

Image Upgrade Progress
----------------------
Mac IP Address AP Class Status Image Info Error Detail
--- --------- -------- ------ ---------- ------------
d8:c7:c8:c4:42:98 10.17.101.1 Orion image-ok image file none
Auto reboot :enable
Use external URL :disable
```

Backing up and Restoring W-IAP Configuration Data

You can back up the W-IAP configuration data and restore the configuration when required.

Viewing Current Configuration

To view the current configuration on the W-IAP:

- In the UI, navigate to **Maintenance** > **Configuration** > **Current Configuration**.
- In the CLI, enter the following command at the command prompt:

```
(Instant AP)# show running-config
```

Backing up Configuration Data

To back up the W-IAP configuration data:

1. Navigate to the **Maintenance > Configuration>** page.
2. Click **Backup Configuration**.
3. Click **Continue** to confirm the backup. The *instant.cfg* containing the W-IAP configuration data is saved in your local file system.
4. To view the configuration that is backed up by the W-IAP, enter the following command at the command prompt:

```
(Instant AP)# show backup-config
```

Restoring Configuration

To restore configuration:

1. Navigate to the **Maintenance > Configuration** page.
2. Click **Restore Configuration**. Click **Browse** to browse your local system and select the configuration file.
3. Click **Restore Now**.
4. Click **Restore Configuration** to confirm restoration. The configuration is restored and the W-IAP reboots to load the new configuration.

Converting a W-IAP to a Remote AP and Campus AP

This section provides the following information:

- Regulatory Domain Restrictions for W-IAP to RAP or CAP Conversion on page 320
- Converting a W-IAP to a Remote AP on page 322
- Converting a W-IAP to a Campus AP on page 323
- Converting a W-IAP to Standalone Mode on page 324
- Converting a W-IAP using CLI on page 325

Regulatory Domain Restrictions for W-IAP to RAP or CAP Conversion

You can provision a W-IAP as a Campus AP or a Remote AP in a controller-based network. Before converting a W-IAP, ensure that there is a regulatory domain match between the W-IAP and controller.

The following table describes the regulatory domain restrictions that apply for the W-IAP to ArubaOS AP conversion:

Table 63: *W-IAP to ArubaOS AP Conversion*

ArubaOS version on Controller	Controller Regulatory Domain	IAP-22x		IAP-27x		W-IAP11x		W-IAP103		All other W-IAPs			
		US	RW	US	RW	US	RW	US	RW	US	Unrestricted	JP	IL
Versions lower than 6.3.0	**US**	–	–	—	—	–	–	—	—	Valid	X	X	X
	Unrestricted	–	–	—	—	–	–	—	—	X	Valid	Valid for JP country code	X
	IL	–	–	—	—	–	–	—	—	X	X	X	Valid
6.3.0	**US**	Valid	X	—	—	–	–	—	—	Valid	X	X	X
	Unrestricted	X	X	—	—	–	–	—	—	X	Valid	Valid for JP country code	X
	IL	X	X	—	—	–	–	—	—	X	X	X	Valid
6.3.1.0, 6.3.1.1, and 6.3.1.2	**US**	Valid	X	—	—	Valid	X	—	—	Valid	X	X	X
	Unrestricted	X	X	—	—	X	X	—	—	X	Valid	Valid for JP country code	X
	IL	X	X	—	—	X	X	—	—	X	X	X	Valid
6.3.1.3	**US**	Valid	X	—	—	Valid	X	—	—	Valid	X	X	X
	Unrestricted	X	Valid	—	—	X	Valid	—	—	X	Valid	Valid for JP country code	X
	IL	X	Valid	—	—	X	Valid	—	—	X	X	X	Valid
6.4 or later	**US**	Valid	X	Valid	X	Valid	X	Valid	X	Valid	X	X	X
	IL	X	Valid	X	Valid	X	Valid	X	Valid	X	Valid	Valid for JP country code	X
	Unrestricted	X	Valid	X	Valid	X	Valid	X	Valid	X	X	X	Valid

NOTE: "**—**" indicates **not supported** and "**X**" indicates **invalid** configuration.
NOTE: The minimum Instant version for W-IAP103 and W-IAP274/275 is 6.4.0.2-4.1.

Converting a W-IAP to a Remote AP

For Remote AP conversion, the Virtual Controller sends the Remote AP convert command to all the other W-IAPs. The Virtual Controller along with the other slave W-IAPs set up a VPN tunnel to the remote controller, and download the firmware through FTP. The Virtual Controller uses IPsec to communicate to the mobility controller over the Internet.

- If the W-IAP obtains W-AirWave information through DHCP (Option 43 and Option 60), it establishes an HTTPS connection to the W-AirWave server and downloads the configuration and operates in the W-IAP mode.
- If the W-IAP does not get W-AirWave information through DHCP provisioning, it tries provisioning through a firmware image server in the cloud by sending a serial number MAC address. If an entry for the W-IAP is present in the firmware image cloud server and is provisioned as a W-IAP > Remote AP, the firmware image cloud server responds with mobility controller IP address, AP group, and AP type. The W-IAP then contacts the controller, establishes certificate-based secure communication, and obtains configuration and image from the controller. The W-IAP reboots and comes up as a Remote AP. The W-IAP then establishes an IPSEC connection with the controller and begins operating in the Remote AP mode.
- If a W-IAP entry for the AP is present in the firmware image cloud server, the W-IAP obtains W-AirWave server information from the cloud server and downloads configuration from W-AirWave to operate in the W-IAP mode.
- If there is no response from the cloud server or AirGroup is received, the W-IAP comes up in Instant mode.
- For more information on firmware image cloud server, see Upgrading a W-IAP on page 317.

A mesh point cannot be converted to Remote AP, because mesh access points do not support VPN connection.

A W-IAP can be converted to a Campus AP and Remote AP only if the controller is running ArubaOS 6.1.4 or later.

The following table describes the supported W-IAP platforms and minimal ArubaOS version required for the Campus AP or Remote AP conversion.

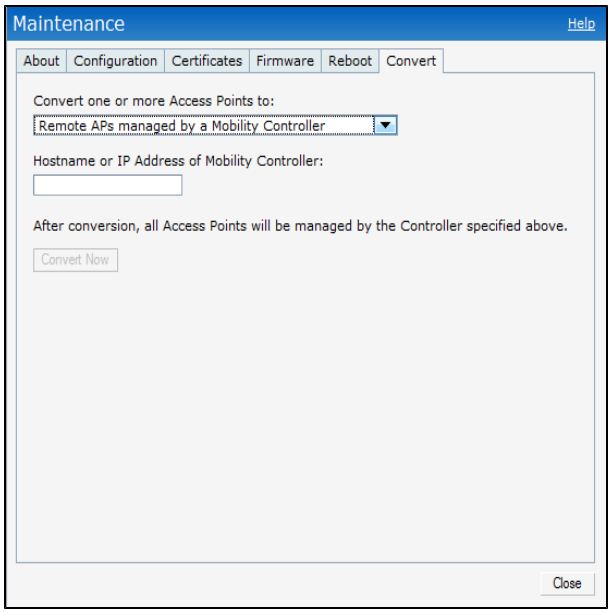
Table 64: *W-IAP Platforms and Minimum ArubaOS Versions for W-IAP to Remote AP Conversion*

W-IAP Platform	ArubaOS Version	Instant Version
W-IAP103	6.4 or later	4.1 or later
W-IAP104	6.1.4 or later	3.0 or later
W-IAP105	6.1.4 or later	1.0 or later
W-IAP134/135	6.1.4 or later	2.0 or later
W-IAP175AC/175P	6.1.4 or later	3.0 or later
W-IAP3WN/3WNP	6.1.4 or later	3.0 or later
W-IAP108/109	6.2.0.0 or later	3.2 or later
W-IAP155/155P	6.3 or later	3.3 or later
W-IAP114/115	6.3.1.1 or later	4.0 or later
W-IAP224/225	6.3.1.1 or later	4.0 or later
W-IAP274/275	6.4 or later	4.1 or later

To convert a W-IAP to a RAP, perform the following steps:

1. Click the **Maintenance** link in the Instant main window.
2. Click the **Convert** tab. The **Convert** tab is displayed.

Figure 121 *Maintenance — Convert Tab*



3. Select **Remote APs managed by a Mobility Controller** from the drop-down list.
4. Enter the hostname (fully qualified domain name) or the IP address of the controller in the **Hostname or IP Address of Mobility Controller** text box. Contact your local network administrator to obtain the IP address.

NOTE

Ensure that the mobility controller IP Address is reachable by the a W-IAPs.

5. Click **Convert Now** to complete the conversion. The W-IAP reboots and begins operating in the Remote AP mode.
6. After conversion, the W-IAP is managed by the Dell Networking W-Series mobility controller.

NOTE

For W-IAPs to function as Remote APs, configure the W-IAP in the Remote AP whitelist and enable the FTP service on the controller.

NOTE

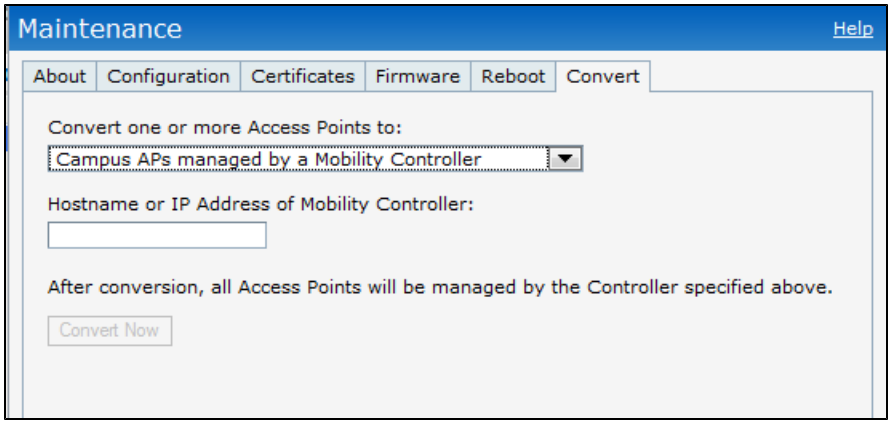
If the VPN setup fails and an error message is displayed, click **OK**, copy the error logs, and share them with your local administrator.

Converting a W-IAP to a Campus AP

To convert a W-IAP to a Campus AP, do the following:

1. Click the **Maintenance** link in the Instant main window.
2. Click the **Convert** tab. The **Convert** tab is displayed.

Figure 122 *Converting a W-IAP to Campus AP*



3. Select **Campus APs managed by a Mobility Controller** from the drop-down list.
4. Enter the hostname, Fully Qualified Domain Name (FQDN), or the IP address of the controller in the **Hostname or IP Address of Mobility Controller** text box. Contact your local administrator to obtain these details.
5. Ensure that the W-IAPs access the mobility controller IP Address.
6. Click **Convert Now** to complete the conversion.

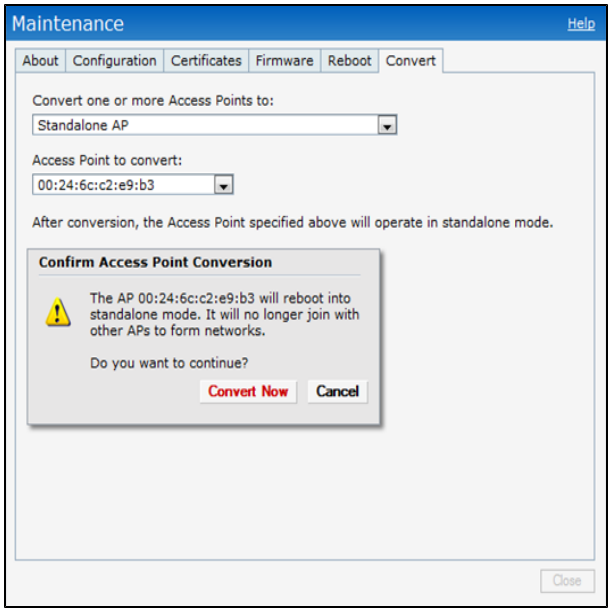
Converting a W-IAP to Standalone Mode

This feature allows you to deploy a W-IAP as an autonomous AP, which is a separate entity from the existing Virtual Controller cluster in the Layer 2 domain.

To convert a W-IAP to a standalone AP:

1. Click the **Maintenance** link in the Instant main window.
2. Click the **Convert** tab. The **Convert** tab is displayed.

Figure 123 *Standalone AP Conversion*



3. Select **Standalone AP** from the drop-down list.
4. Select the Access Point from the drop-down list.
5. Click **Convert Now** to complete the conversion. The a W-IAP now operates in the standalone mode.

Converting a W-IAP using CLI

To convert a W-IAP

```
(Instant AP)# convert-aos-ap <mode> <controller-IP-address>
```

Resetting a Remote AP or Campus AP to a W-IAP

The reset button located on the rear of a W-IAP can be used to reset the W-IAP to factory default settings.

To reset a W-IAP, perform the following steps:

1. Power off the W-IAP.
2. Press and hold the reset button using a small and narrow object such as a paperclip.
3. Power on the W-IAP without releasing the reset button. The power LED flashes within 5 seconds indicating that the reset is completed.
4. Release the reset button. The W-IAP reboots with the factory default settings.

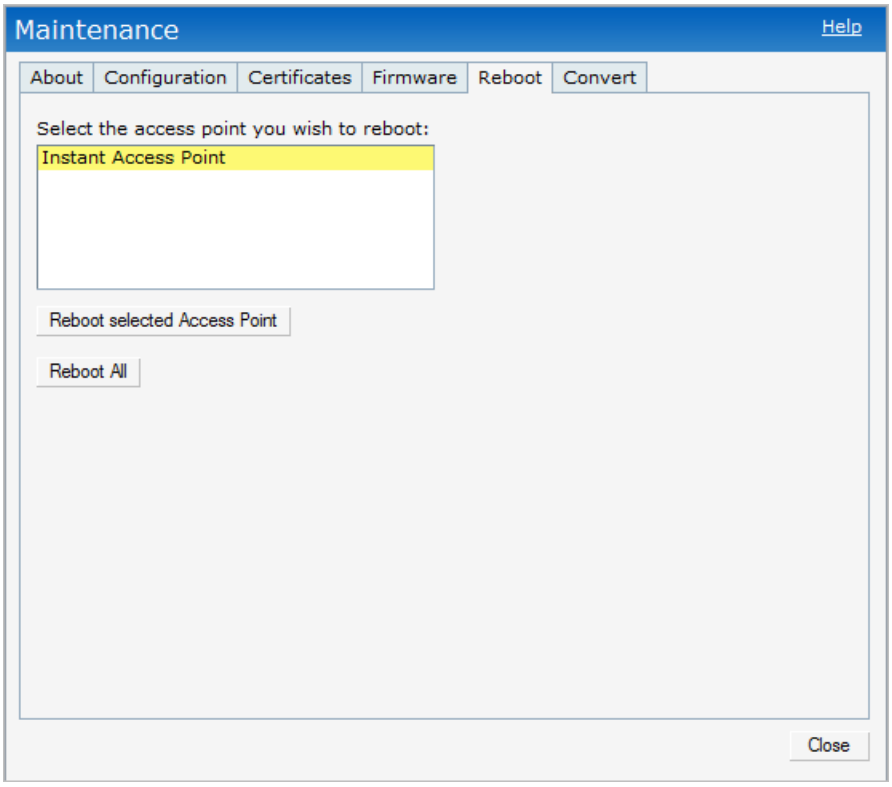
All APs have a reset button, except IAP-175P/175AC. Contact Dell support for resetting these W-IAPs.

Rebooting the W-IAP

If you encounter any problem with the W-IAPs, you can reboot all W-IAPs or a selected W-IAP in a network using the Instant UI. To reboot a W-IAP:

1. Click the **Maintenance** link. The **Maintenance** window is displayed.
2. Click the **Reboot** tab.

Figure 124 *Rebooting the W-IAP*



3. In the W-IAP list, select the W-IAP that you want to reboot and click **Reboot selected Access Point**. To reboot all the W-IAPs in the network, click **Reboot All.**
4. The **Confirm Reboot for AP** message is displayed. Click **Reboot Now** to proceed. The **Reboot in Progress** message is displayed indicating that the reboot is in progress. The **Reboot Successful** message is displayed after the process is complete. If the system fails to boot, the **Unable to contact Access Points after reboot was initiated message** is displayed.
5. Click **OK**.

This chapter provides the following information:

- Configuring SNMP on page 327
- Configuring a Syslog Server on page 330
- Configuring TFTP Dump Server on page 332
- Running Debug Commands from the UI on page 333

Configuring SNMP

This section provides the following information:

- SNMP Parameters for W-IAP on page 327
- Configuring SNMP on page 328
- Configuring SNMP Traps on page 330

SNMP Parameters for W-IAP

Instant supports SNMPv1, SNMPv2c, and SNMPv3 for reporting purposes only. A W-IAP cannot use SNMP to set values in a Dell system.

You can configure the following parameters for a W-IAP:

Table 65: *SNMP Parameters for W-IAP*

Field	Description
Community Strings for SNMPV1 and SNMPV2	An SNMP Community string is a text string that acts as a password, and is used to authenticate messages sent between the Virtual Controller and the SNMP agent.
If you are using SNMPv3 to obtain values from the W-IAP, you can configure the following parameters:	
Name	A string representing the name of the user.
Authentication Protocol	An indication of whether messages sent on behalf of this user can be authenticated, and if so, the type of authentication protocol used. This can take one of the two values: • MD5– HMAC-MD5-96 Digest Authentication Protocol • SHA: HMAC-SHA-96 Digest Authentication Protocol
Authentication protocol password	If messages sent on behalf of this user can be authenticated, the (private) authentication key for use with the authentication protocol. This is a string password for MD5 or SHA depending on the choice above.
Privacy protocol	An indication of whether messages sent on behalf of this user can be protected from disclosure, and if so, the type of privacy protocol which is used. This takes the value DES (CBC-DES Symmetric Encryption).
Privacy protocol password	If messages sent on behalf of this user can be encrypted/decrypted with DES, the (private) privacy key for use with the privacy protocol.

Configuring SNMP

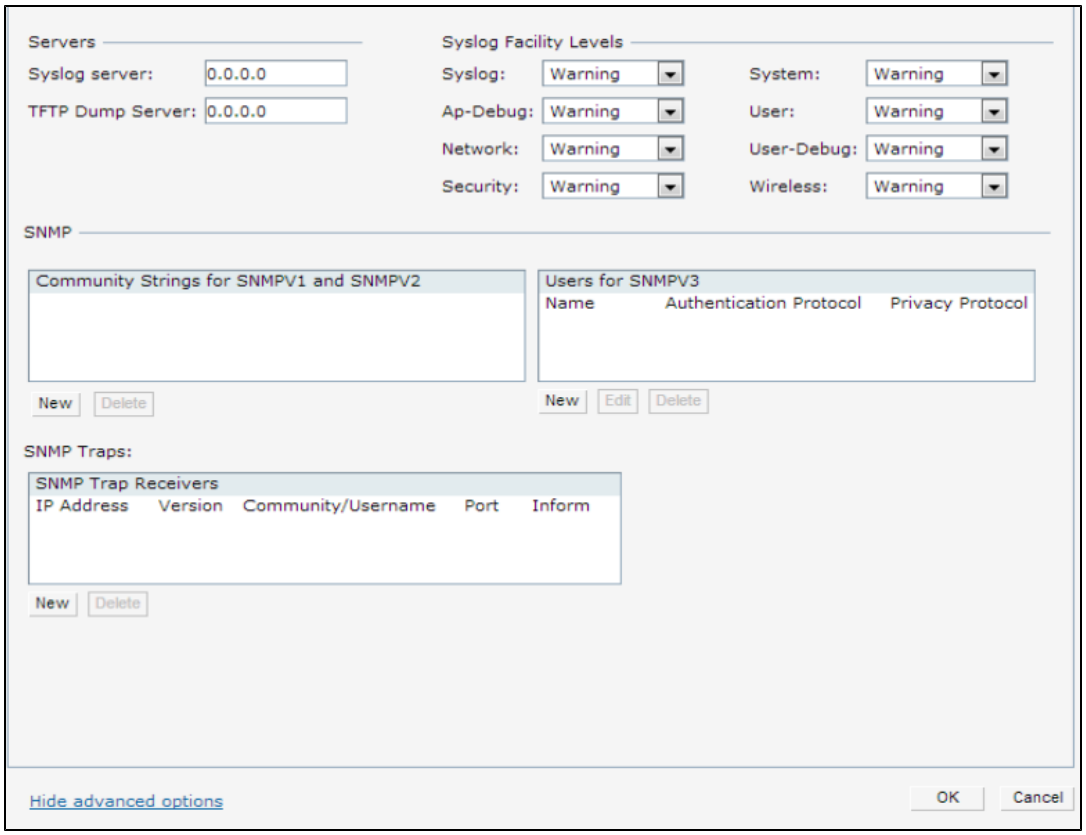
This section describes the procedure for configuring SNMPv1, SNMPv2, and SNMPv3 community strings using the Instant UI or CLI.

Creating community strings for SNMPv1 and SNMPv2 Using Instant UI

To create community strings for SNMPv1 and SNMPv2:

1. Click the **System** link at the top right corner of the Instant main window. The system window is displayed.
2. Click the **Monitoring** tab. The following figure shows the SNMP configuration parameters displayed in the **Monitoring** tab.

Figure 125 *Monitoring Tab: SNMP Configuration Parameters*



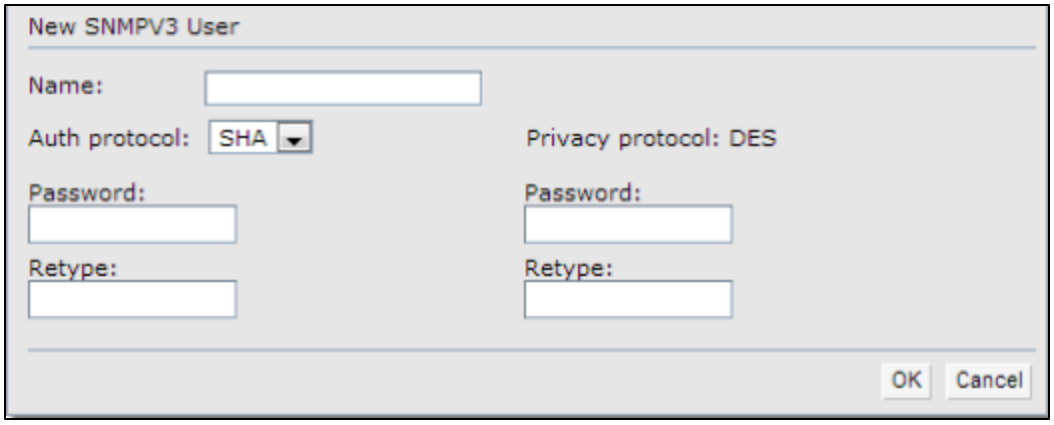
3. Click **New**.
4. Enter the string in the **New Community String** text box.
5. Click **OK**.
6. To delete a community string, select the string, and click **Delete**.

Creating community strings for SNMPv3 Using Instant UI

To create community strings for SNMPv3:

1. Click **System** link at the top right corner of the Instant main window. The system window is displayed.
2. Click the **Monitoring** tab. The SNMP configuration parameters displayed in the **Monitoring** tab.
3. Click **New** in the **Users for SNMPV3** box. A window for specifying SNMPv3 user information is displayed.

Figure 126 *SNMPv3 User*



4. Enter the name of the user in the **Name** text box.
5. Select the type of authentication protocol from the **Auth protocol** drop-down list.
6. Enter the authentication password in the **Password** text box and retype the password in the **Retype** text box.
7. Select the type of privacy protocol from the **Privacy protocol** drop-down list.
8. Enter the privacy protocol password in the **Password** text box and retype the password in the **Retype** text box.
9. Click **OK**.
10. To edit the details for a particular user, select the user and click **Edit**.
11. To delete a particular user, select the user and click **Delete**.

Configuring SNMP Community Strings in the CLI

To configure an SNMP engine ID and host:

```
(Instant AP)(config)# snmp-server engine-id <engine-ID>
(Instant AP)(config)# host <ipaddr> version {1 <name> udp-port <port>}|{2c|3 <name> [inform]
[udp-port <port>]}
```

To configure SNMPv1 and SNMPv2 community strings:

```
(Instant AP)(config)# snmp-server community <password>
```

To configure SNMPv3 community strings:

```
(Instant AP)(config)# snmp-server user <name> <auth-protocol> <password> <privacy-protocol>
<password>
```

To view SNMP configuration:

```
(Instant AP)# show snmp-configuration

Engine ID:D8C7C8C44298
Community Strings
-----------------
Name
----
SNMPv3 Users
------------
Name Authentication Type Encryption Type
---- ------------------- ---------------
SNMP Trap Hosts
---------------
IP Address Version Name Port Inform
---------- ------- ---- ---- ------
```

Configuring SNMP Traps

Instant supports the configuration of external trap receivers. Only the W-IAP acting as the Virtual Controller generates traps. The traps for W-IAP cluster are generated with Virtual Controller IP as the source IP if Virtual Controller IP is configured. The OID of the traps is 1.3.6.1.4.1.14823.2.3.3.1.200.2.X.

You can configure SNMP traps using the Instant UI or CLI.

In the Instant UI

To configure an SNMP trap receiver:

1. Navigate to **System** > **Show advanced options** > **Monitoring**. The **Monitoring** window is displayed.
2. Under **SNMP Traps**, enter a name in the **SNMP Engine ID** text box. It indicates the name of the SNMP agent on the access point. The SNMPV3 agent has an engine ID that uniquely identifies the agent in the device and is unique to that internal network.
3. Click **New** and update the following fields:
   - **IP Address–** Enter the **IP Address** of the new SNMP Trap receiver.
   - **Version**– Select the SNMP version– **v1, v2c, v3** from the drop-down list. The version specifies the format of traps generated by the access point.
   - **Community/Username**– Specify the community string for SNMPv1 and SNMPv2c traps and a username for SNMPv3 traps.
   - **Port**– Enter the port to which the traps are sent. The default value is 162.
   - **Inform**– When enabled, traps are sent as SNMP INFORM messages. It is applicable to SNMPv3 only. The default value is **Yes**.
4. Click **OK** to view the trap receiver information in the **SNMP Trap Receivers** window.

In the CLI

To configure SNMP traps:

```
(Instant AP)(config)# snmp-server host <IP-address> {version 1 | version 2 | version 3} <name>
udp-port <port> inform
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Instant supports SNMP Management Information Bases (MIBs) along with Dell-MIBs. For information about MIBs and SNMP traps, see *Dell Networking W-Series Instant MIB Reference Guide*.

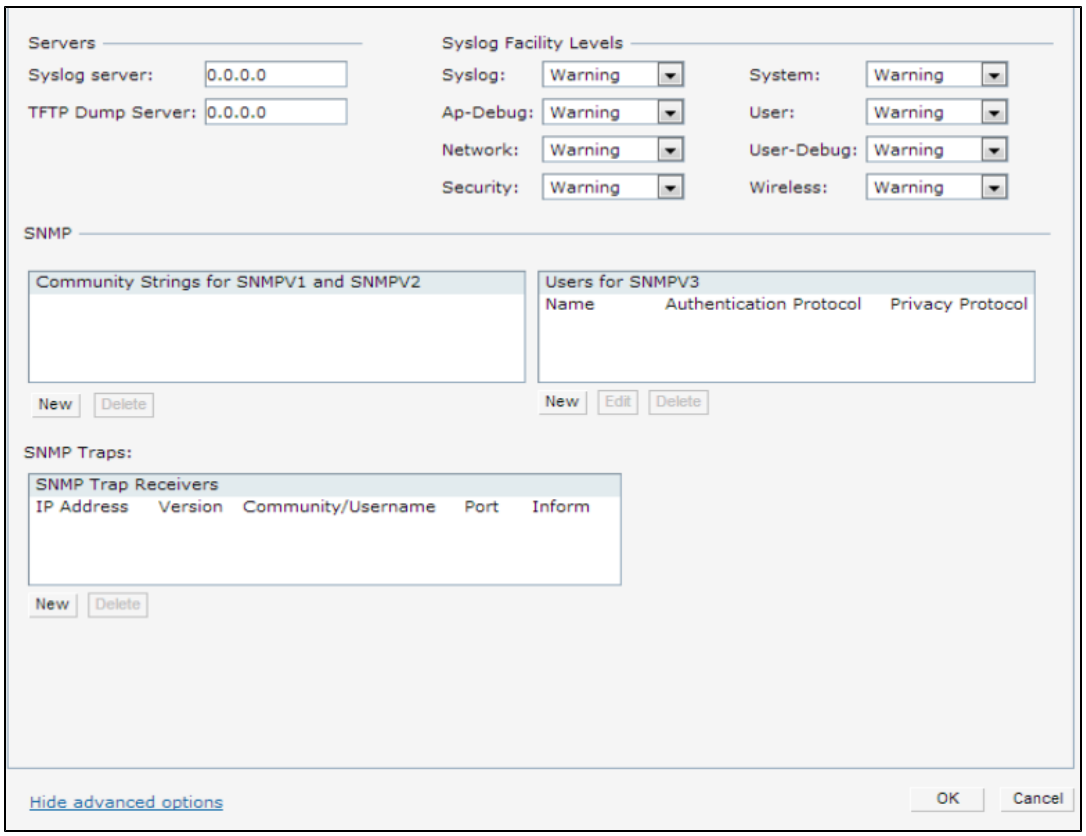
Configuring a Syslog Server

You can specify a syslog server for sending syslog messages to the external servers either by using the Instant UI or CLI.

In the Instant UI

1. In the Instant main window, click the **System** link. The **System** window is displayed.
2. Click **Show advanced options** to display the advanced options.
3. Click the **Monitoring** tab. The **Monitoring** tab details are displayed.

Figure 127 *Syslog Server*



4. In the **Syslog server** text box, enter the IP address of the server to which you want to send system logs.
5. Select the required values to configure syslog facility levels. Syslog Facility is an information field associated with a syslog message. It is an application or operating system component that generates a log message. The following seven facilities are supported by Syslog:

- **AP-Debug–** Detailed log about the AP device.
- **Network–** Log about change of network, for example, when a new W-IAP is added to a network.
- **Security–** Log about network security, for example, when a client connects using wrong password.
- **System–** Log about configuration and system status.
- **User–** Important logs about client.
- **User-Debug–** Detailed log about client.
- **Wireless–** Log about radio.

The following table describes the logging levels in order of severity, from the most to the least severe.

Table 66: *Logging Levels*

Logging Level	Description
Emergency	Panic conditions that occur when the system becomes unusable.
Alert	Any condition requiring immediate attention and correction.
Critical	Any critical conditions such as a hard drive error.
Errors	Error conditions.

Logging Level	Description
Warning	Warning messages.
Notice	Significant events of a non-critical and normal nature. The default value for all Syslog facilities.
Informational	Messages of general interest to system users.
Debug	Messages containing information useful for debugging.

6. Click **OK**.

In the CLI

To configure a syslog server:

```
(Instant AP)(config)# syslog-server <IP-address>
```

To configure syslog facility levels:

```
(Instant AP)(config)# syslog-level <logging-level>[ap-debug |network |security |system |user |
user-debug | wireless]
(Instant AP)(config)# end
(Instant AP)# commit apply
```

To view syslog logging levels:

```
Instant Access Point# show syslog-level

Logging Level
-------------
Facility Level
-------- -----
ap-debug warn
network warn
security warn
system warn
user warn
user-debug warn
wireless error
```

Configuring TFTP Dump Server

You can configure a TFTP server for storing core dump files by using the Instant UI or CLI.

In the Instant UI

1. In the Instant main window, click the **System** link. The **System** window is displayed.
2. Click **Show advanced options** to display the advanced options.
3. Click the **Monitoring** tab. The **Monitoring** tab details are displayed.
4. Enter the IP address of the TFTP server in the **TFTP Dump Server** text box.
5. Click **OK**.

In the CLI

To configure a TFTP server:

```
(Instant AP)(config)# tftp-dump-server <IP-address>
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Running Debug Commands from the UI

To run the debugging commands from the UI:

1. Navigate to **More**>**Support** at the top right corner of the Instant main window. The **Support** window is displayed.
2. Select the required option from the **Command** drop-down list.
3. Select **All Access Points** or **Instant Access Point(VC)** from the **Target** drop-down list.
4. Click **Run**. When you run debug commands and click **Save**, the output of all the selected commands is displayed in a single page.

Support Commands

You can view the following information for each access point in the cluster using the support window:

- **AP 3G/4G Status**– Displays the cellular status of the W-IAP.
- **AP 802.1x Certificate**– Displays the CA certificate and server certificate for the Virtual Controller.
- **AP 802.1X Statistics**– Displays the 802.1X statistics of the W-IAP.
- **AP Access Rule Table**– Displays the list of ACL rules configured on the W-IAP.
- **AP Inbound Firewall Rules**–Displays inbound firewall rules configured on the W-IAP
- **AP Active**– Displays the list of active APs in Instant network.
- **AP Airgroup Cache**– Displays the Bonjour Multicast DNS (mDNS) records for the W-IAP.
- **AP Airgroup CPPM Entries**– Displays the AirGroup CPPM policies of the registered devices.
- **AP Airgroup CPPM Servers**– Displays the AirGroup CPPM server information.
- **AP Airgroup Debug Statistics–** Displays the debug statistics for the W-IAP.
- **AP Airgroup Servers**– Displays information about the Bonjour devices which supports AirPrint and AirPlay services for the W-IAP.
- **AP Airgroup User**– Displays the IP/MAC address, device name, VLAN, type of connection of the Bonjour devices for the W-IAP.
- **AP Allowed Channels**– Displays information of the allowed channels for the W-IAP.
- **AP Allowed MAX-EIRP–** Displays information on the maximum EIRP settings that can be configured on a W-IAP serving in a specific regulatory domain.
- **AP All Supported Timezones**– Displays all the supported time zones of Instant.
- **AP ARM Bandwidth Management**– Displays bandwidth management information for the W-IAP.
- **AP ARM Channels**– Displays ARM channel details for the W-IAP.
- **AP ARM Configuration**– Displays ARM configuration details for the W-IAP.
- **AP ARM History**– Displays the channel history and power changes due to Adaptive Radio Management (ARM) for the W-IAP.
- **AP ARM Neighbors**– Displays the ARM neighbors of the W-IAP.
- **AP ARM RF Summary**– Displays the status and statistics for all channels monitored by the W-IAP.
- **AP ARM Scan Times**– Displays channel scanning information for the W-IAP.
- **AP ARP Table**– Displays the ARP table of the W-IAP.
- **AP Association Table**– Displays information about the W-IAP association.
- **AP Auth-Survivability cache**– Displays the list of 802.1X cached user's information.
- **AP Authentication Frames**– Displays the authentication trace buffer information of the W-IAP.
- **AP BSSID Table**– Displays the Basic Service Set (BSS) table of the W-IAP.
- **AP Captive Portal Domains**–Displays captive portal domains configured on the W-IAP.

- **AP Captive Portal Auto White List**–Displays details about the automatic whitelist configured for a captive portal profile.
- **AP Checksum**–Displays checksum details for a W-IAP.
- **AP Client Match Action**–Displays details of the client match action.
- **AP Client Match Live**– Displays the live details of the client match configuration on a W-IAP.
- **AP Client Match History**– Displays the historical details of the client match configuration on a W-IAP.
- **AP Client Match Status**– Displays information about the client match configuration status.
- **AP Client Match Triggers**–Displays information about the client match triggers.
- **AP Client Table**–Displays the client details.
- **AP Client View** – Displays client details of a W-IAP.
- **AP Country Codes**– Displays country code details for the W-IAP.
- **AP CPU Details**– Displays detailed information about memory utilization and CPU load for system processes.
- **AP CPU Utilization**– Displays utilization of CPU for the W-IAP.
- **AP Crash Info**– Displays crash log information (if it exists) for the W-IAP. The stored information is cleared from the flash after the AP reboots.
- **AP Current Time**– Displays the current time configured on the W-IAP.
- **AP Current Timezone**– Displays the current time zone configured on the W-IAP.
- **AP Datapath ACL Table Allocation**– Displays ACL table allocation details for the W-IAP.
- **AP Datapath ACL Tables–** Displays the list of ACL rules configured for the SSID and Ethernet port profiles.
- **AP Datapath Bridge Table**– Displays bridge table entry statistics including MAC address, VLAN, assigned VLAN, Destination and flag information for the W-IAP.
- **AP Datapath DMO Session**– Displays details of a DMO session.
- **AP Datapath Dns Id Map**– Displays the mapping details for the DNS ID.
- **AP Datapath DPI Session Table** and **AP Datapath DPI Session Table Verbose**–Display the datapath session table entries.
- **AP Datapath Multicast Table**– Displays multicast table statistics for the W-IAP.
- **AP Datapath Nat Pool**–Displays NAT pool details configured in the datapath.
- **AP Datapath Route Table–** Displays route table statistics for the W-IAP.
- **AP Datapath Session Table–** Displays the datapath session table statistics for the W-IAP.
- **AP Datapath Statistics–** Displays the hardware packet statistics for the W-IAP.
- **AP Datapath User Table–** Displays datapath user statistics such as current entries, pending deletes, high water mark, maximum entries, total entries, allocation failures, invalid users, and maximum link length for the W-IAP.
- **AP Datapath VLAN Table–** Displays the VLAN table information such as VLAN memberships inside the datapath including L2 tunnels for the W-IAP.
- **AP Daylight Saving Time**–Displays the Daylight Saving Time configured on the W-IAP.
- **AP Derivation Rules**–Displays the role and VLAN derivation rules configured on a W-IAP.
- **AP DPI Debug statistics**–Displays DPI statistics that can be used for debugging DPI issues.
- **AP Driver Configuration–** Displays driver configuration details of the W-IAP.
- **AP Election** and **AP Election Statistics**–Display the master election statistics.
- **AP Environment Variable**– Displays information about the type of antenna used by the W-IAP.
- **AP ESSID Table–** Displays the SSID profiles configured on the W-IAP.
- **AP Flash Configuration–** Displays statistics of the W-IAP configuration stored in flash memory.
- **AP IGMP Group Table**–Displays IGMP group information.

- **AP IAP-VPN Retry Counters**–Displays IAP-VPN tunnel details.
- **AP Interface Counters–** Displays information about the Ethernet interface packet counters for the W-IAP.
- **AP Interface Status–** Displays the Ethernet port status for the W-IAP.
- **AP Internal DHCP Status**–Displays details on DHCP allocation.
- **AP IP Interface**–Displays a summary of all IP-related information for Ethernet interfaces configured on the W-IAP.
- **AP IP Route Table–** Displays information about IP routes for the W-IAP.
- **AP L3 Mobility Datapath**–Display L3 mobility details.
- **AP L3 Mobility Events Log**–Displays a log with L3 client roaming details.
- **AP L3 Mobility Status**–Displays the status of L3 roaming clients.
- **AP LACP Status**–Displays the Link Aggregation Control Protocol (LACP) configuration status.
- **AP Log All–** Displays all logs for the W-IAP.
- **AP Log AP-Debug–** Displays logs with debugging information for the W-IAP.
- **AP Log Conversion**–Displays image conversion details for the W-IAP.
- **AP Log Driver**–Displays the status of drivers configured on the W-IAP.
- **AP Log Kernel**–Displays logs for AP's kernel.
- **AP Log Network–** Displays network logs for the W-IAP.
- **AP Log PPPd**–Displays the Point-to-Point Protocol daemon (PPPd) network connection details.
- **AP Log Rapper**–Displays rapper information.
- **AP Log Sapd**– Displays SAPd logs.
- **AP Log Security**– Displays security logs of the W-IAP.
- **AP Log System**– Displays system logs of the W-IAP.
- **AP Log Tunnel Status Management**–Displays tunnel status.
- **AP Log Upgrade**–Displays image download and upgrade details for the W-IAP.
- **AP Log User-Debug**– Displays user-debug logs of the W-IAP.
- **AP Log User**– Displays user logs of the W-IAP.
- **AP Log VPN Tunnel Log–** Displays VPN tunnel status for the W-IAP.
- **AP Log Wireless**– Displays wireless logs of the W-IAP.
- **AP Management Frames**– Displays the traced 802.11 management frames for the W-IAP.
- **AP Memory Allocation State Dumps**– Displays the memory allocation details for the W-IAP.
- **AP Memory Utilization**– Displays memory utilization of the W-IAP.
- **AP Mesh Counters**– Displays the mesh counters of the W-IAP.
- **AP Mesh Link**– Displays the mesh link of the W-IAP.
- **AP Mesh Neighbors**– Displays the mesh link neighbors of the W-IAP.
- **AP Monitor Active Laser Beams**– Displays the active laser beam sources for the W-IAP.
- **AP Monitor AP Table**– Displays the list of APs monitored by the W-IAP.
- **AP Monitor ARP Cache**– Displays ARP cache details for the W-IAP.
- **AP Monitor Client Table**– Displays the list of clients monitored by the W-IAP.
- **AP Monitor Containment Information**– Displays containment details for the W-IAP.
- **AP Monitor Potential AP Table**– Displays the list of potential APs for the W-IAP.
- **AP Monitor Potential Client Table**– Displays the list of potential clients for the W-IAP.
- **AP Monitor Router**– Displays information about the potential wireless devices.
- **AP Monitor Scan Information**– Displays scanned information for the W-IAP.

- **AP Monitor Status**– Displays the configuration and status of monitor information of the W-IAP.
- **AP Persistent Clients**– Displays the list persistent clients for the W-IAP.
- **AP PMK Cache**– Displays the PMK cache details for the clients associated with the W-IAP.
- **AP PPPoE uplink debug**– Displays PPPoE debug logs.
- **AP PPPoE uplink status**– Displays PPPoE uplink status.
- **AP Processes**– Displays the processes running on the W-IAP.
- **AP Radio 0 Stats**– Displays aggregate debug statistics of the W-IAP Radio 0.
- **AP Radio 1 Stats**– Displays aggregate debug statistics of the W-IAP Radio 1. .
- **AP Radio 0 Client Probe Report**– Displays a report on the AP clients connected to W-IAP Radio 0.
- **AP Radio 1 Client Probe Report**– Displays a report on the AP clients connected to W-IAP Radio 1.
- **AP RADIUS Statistics**– Displays the RADIUS server statistics for the W-IAP.
- **AP Shaping Table**– Displays shaping information for clients associated with the W-IAP.
- **AP Sockets**– Displays information sockets of the W-IAP.
- **AP STM Configuration**– Displays STM configuration details for each SSID profile configured on the W-IAP.
- **AP System Status**– Displays detailed system status information for the W-IAP.
- **AP System Summary**– Displays the W-IAP configuration.
- **AP Swarm State**– Displays details of the W-IAP cluster to which the AP is connected.
- **AP Tech Support Dump**– Displays the logs with complete W-IAP configuration information required for debugging by technical support.
- **AP Tech Support Dump Advanced**– Displays the logs with advanced configuration details and logs required for debugging by technical support.
- **AP Uplink Status**– Displays uplink status for the W-IAP.
- **AP User Table**– Displays the list of clients for the W-IAP.
- **AP Valid Channels**– Displays valid channels of the W-IAP.
- **AP Version**– Displays the version number of the W-IAP.
- **AP VPN Status**– Displays VPN status for the W-IAP.
- **AP Virtual Beacon Report**– Displays a report on virtual beacons for a W-IAP.
- **AP Wired Port Settings**– Displays wired port configuration details for the W-IAP.
- **AP Wired User Table**– Displays the list of clients associated with the wired network profile configured on the W-IAP.
- **VC About**– Displays information such as AP type, build time of image, and image version for the Virtual Controller.
- **VC Active Configuration**– Displays the active configuration of Virtual Controller.
- **VC Airgroup Service**– Displays the Bonjour services supported by the Virtual Controller.
- **VC Airgroup Status**– Displays the status of the AirGroup and CPPM server details configured on the Virtual Controller.
- **VC Allowed AP Table**– Displays the list of allowed APs.
- **VC AMP Current State Data**– Displays the current status of W-AirWave Management Platform.
- **VC AMP Current Stats Data**– Displays the current W-AirWave configuration details.
- **VC AMP Data Sent**– Displays information about the data exchange between W-AirWave server and the Virtual Controller.
- **VC AMP Events Pending**– Displays information about the pending events on the W-AirWave server.
- **VC AMP Last Configuration Received**– Displays the last configuration details received from W-AirWave.

- **VC AMP Single Sign-on Key**– Displays single sign-on key details for W-AirWave.
- **VC Application Services**– Displays the details of application services, which includes protocol number, port number.
- **VC DHCP Option 43 Received**– Displays information about the current activities for the DHCP scope with Option 43.
- **VC Global Alerts**– Displays the list of alerts for all W-IAPs managed by the Virtual Controller.
- **VC Global Statistics**– Displays the flow information and signal strength of the Virtual Controller.
- **VC IDS AP List**– Displays the list of W-IAPs monitored by the Virtual Controller.
- **VC IDS Client List**– Displays the list of clients detected by IDS for the Virtual Controller.
- **VC Internal DHCP Server Configuration**– Displays the configuration details of the internal DHCP server.
- **VC L2TPv3 config**– Displays the L2TPv3 configuration status.
- **VC L2TPv3 tunnel status**– Displays the L2TPv3 tunnel status.
- **VC L2TPv3 tunnel configuration**– Displays the L2TPv3 tunnel configuration status.
- **VC L2TPv3 session status**– Displays the L2TPv3 session configuration status.
- **VC L2TPv3 system wide global statistics**– Displays the L2TPv3 system statistics.
- **VC Local User Database**– Displays the list of users configured for the W-IAP.
- **VC OpenDNS Configuration and Status**– Displays configuration details and status of the OpenDNS server.
- **VC Radius Attributes**– Displays information about the RADIUS attributes.
- **VC Radius Servers**– Displays the list of RADIUS servers configured on the W-IAP.
- **VC Saved Configuration**– Displays the configuration details of the Virtual Controller.
- **VC Scanning Statistics**– Displays the scanned information for the W-IAP.
- **VC SNMP Configuration**– Displays the SNMP configuration details of the W-IAP.
- **VC Uplink 3G/4G Configuration**– Displays the 3G/4G cellular configuration information for the W-IAPs managed by the Virtual Controller.
- **VC Uplink Management Configuration**– Displays uplink configuration details for the Virtual Controller.
- **VC WISPr Configuration**– Displays the WISPr configuration details.

Use the support commands under the supervision of Dell technical support.

This chapter describes the following procedures:

- Understanding Hotspot Profiles on page 338
- Configuring Hotspot Profiles on page 339
- Sample Configuration on page 349

In the current release, Instant supports the hotspot profile configuration only through the CLI.

Understanding Hotspot Profiles

Hotspot 2.0 is a Wi-Fi Alliance specification based on the 802.11u protocol, which allows wireless clients to discover hotspots using management frames (such as beacon, association request, and association response), connect to networks, and roam between networks without additional authentication.

The Hotspot 2.0 provides the following services:

- Network discovery and selection– Allows the clients to discover suitable and available networks by advertising the access network type, roaming consortium, and venue information through the management frames. For network discovery and selection, Generic Advertisement Service (GAS) and Access Network Query Protocol (ANQP) are used.
- QOS Mapping– Provides a mapping between the network-layer QoS packet marking and over- the-air QoS frame marking based on user priority.

When a hotspot is configured in a network:

- The clients search for available hotspots using the beacon management frame.
- When a hotspot is found, the client sends queries to obtain information about the type of network authentication and IP address, and IP address availability using the Generic Advertisement Service (GAS) action frames.
- Based on the response of the advertisement Server (response to the GAS Action Frames), the relevant hotspot is selected and the client attempts to associate with it.
- Based on the authentication mode used for mobility clients, the client authenticates to access the network.

Generic Advertisement Service (GAS)

GAS is a request-response protocol, which provides L2 transport mechanism between a wireless client and a server in the network prior to authentication. It helps in determining an 802.11 infrastructure before associating clients and allows clients to send queries to multiple 802.11 networks in parallel.

An AP can include its service provider Organization Identifier (OI) indicating the service provider identity in beacons and probe responses to clients. When a client recognizes a W-IAP's OI, it attempts to associate to that W-IAP using the security credentials corresponding to that service provider. If the client does not recognize the AP’s OI, the client sends a Generic Advertisement Service (GAS) query to the W-IAP to request more information about the network before associating. A client transmits a GAS Query using a GAS Initial Request frame and the W-IAP provides the query response or information on how to receive the query response in a GAS Initial Response frame. To transmit a GAS query for any advertisement protocol, the advertisement protocol ID must include the advertisement protocol information element with information about the advertisement protocol and its corresponding advertisement control.

Access Network Query Protocol (ANQP)

ANQP provides a range of information, such as IP address type and availability, roaming partners accessible through a hotspot, and the Extensible Authentication Protocol (EAP) method supported for authentication, for a query and response protocol. The ANQP Information Elements (IEs) provide additional data that can be sent from a W-IAP to the client to identify the W-IAP's network and service provider. If a client requests this information through a GAS query, the hotspot AP sends the ANQP capability list in the GAS Initial Response frame indicating support for the following IEs:

- Venue Name
- Domain Name
- Network Authentication Type
- Roaming Consortium List
- Network Access Identifier Realm
- 3GPP Cellular Network Data

Hotspot 2.0 Query Protocol (H2QP)

The H2QP profiles provide a range of information on hotspot 2.0 elements such as hotspot protocol and port, operating class, operator names, WAN status, and uplink and downlink metrics.

Information Elements (IEs) and Management Frames

The hotspot 2.0 configuration supports the following IEs:

- Interworking IE—Provides information about the Interworking service capabilities such as the Internet availability in a specific service provider network.
- Advertisement Protocol IE—Provides information about the advertisement protocol that a client can use for communication with the advertisement servers in a network.
- Roaming Consortium IE—Provides information about the service provider network for roaming clients, which can be used to authenticate with the AP.

The IEs are included in the following Management Frames when 802.11u is enabled:

- Beacon Frame
- Probe Request Frame
- Probe response frame
- Association Request
- Re-Association request

NAI Realm List

An NAI Realm profile identifies and describes a NAI realm to which the clients can connect. The NAI realm settings on a W-IAP as an advertisement profile to determine the NAI realm elements that must be included as part of a GAS Response frame.

Configuring Hotspot Profiles

To configure a hotspot profile, perform the following steps:

1. Create the required ANQP and H2QP advertisement profiles.
2. Create a hotspot profile.

3. Associate the required ANQP and H2QP advertisement profiles created in step 1 to the hotspot profile created in step 2.
4. Create a SSID Profile with enterprise security and WPA2 encryption settings and associate the SSID with the hotspot profile created in step 2.

Creating Advertisement Profiles for Hotspot Configuration

A hotspot profile contains one or several advertisement profiles. The following advertisement profiles can be configured through the Instant CLI:

- ANQP advertisement profiles
  - NAI Realm profile
  - Venue Name Profile
  - Network Authentication Profile
  - Roaming Consortium Profile
  - 3GPP Profile
  - IP Address availability Profile
  - Domain Name Profile
- H2QP advertisement profiles
  - Operator Friendly Name Profile
  - Connection Capability Profile
  - Operating Class Profile
  - WAN-Metrics Profile

Configuring an NAI Realm Profile

You configure a Network Access Identifier (NAI) Realm profile to define the NAI realm information, which can be sent as an ANQP IE in a GAS query response.

To configure a NAI profile, enter the following commands at the command prompt:

```
(Instant AP)(config)# hotspot anqp-nai-realm-profile <name>
(Instant AP)(nai-realm <name>)# nai-realm-name <name>
(Instant AP)(nai-realm <name>)# nai-realm-encoding {<utf8>|<rfc4282>}
(Instant AP)(nai-realm <name>)# nai-realm-eap-method <eap-method>
(Instant AP)(nai-realm <name>)# nai-realm-auth-id-1 <authentication-ID>
(Instant AP)(nai-realm <name>)# nai-realm-auth-id-2 <authentication-ID>
(Instant AP)(nai-realm <name>)# nai-realm-auth-value-1 <authentication-value>
(Instant AP)(nai-realm <name>)# nai-realm-auth-value-2 <authentication-value>
(Instant AP)(nai-realm <name>)# nai-home-realm
(Instant AP)(nai-realm <name>)# enable
(Instant AP)(nai-realm <name>)# end
(Instant AP)# commit apply
```

You can specify any of the following EAP methods for the **nai-realm-eap-method <eap-method>** command:

- **identity**– To use EAP Identity type. The associated numeric value is 1.
- **notification**–To allow the hotspot realm to use EAP Notification messages for authentication. The associated numeric value is 2.
- **one-time-password**–To use Authentication with a single-use password. The associated numeric value is 5.
- **generic-token-card**–To use EAP Generic Token Card (EAP-GTC). The associated numeric value is 6.
- **eap-tls**–To use EAP-Transport Layer Security. The associated numeric value is 13.
- **eap-sim**–To use EAP for GSM Subscriber Identity Modules. The associated numeric value is 18.

- **eap-ttls**–To use EAP-Tunneled Transport Layer Security. The associated numeric value is 21.
- **peap**–To use protected Extensible Authentication Protocol. The associated numeric value is 25.
- **crypto-card**– To use crypto card authentication. The associated numeric value is 28.
- **peapmschapv2**– To use PEAP with Microsoft Challenge Handshake Authentication Protocol version 2 (MSCHAPV2). The associated numeric value is 29.
- **eap-aka**–To use EAP for UMTS Authentication and Key Agreement. The associated numeric value is 50.

The following table lists the possible authentication IDs and their respective values:

Table 67: *NAI Realm Profile Configuration Parameters*

Authentication ID	Authentication Value
reserved • Uses the reserved authentication method. • The associated numeric value is **0**.	–
expanded-eap • Uses the expanded EAP authentication method. • The associated numeric value is **1**.	Use expanded-eap as the authentication value.
non-eap-inner-auth • Uses non-EAP inner authentication type. • The associated numeric value is **2**.	The following authentication values apply: • **reserved**– The associated numeric value is **0**. • **pap**–The associated numeric value is **1**. • **chap**–The associated numeric value is **2**. • **mschap**–The associated numeric value is **3**. • **mschapv2**–The associated numeric value is **4**.
eap-inner-auth • Uses EAP inner authentication type. • The associated numeric value is **3**.	The following authentication values apply: • **reserved**– The associated numeric value is **0**. • **pap**–The associated numeric value is **1**. • **chap**–The associated numeric value is **2**. • **mschap**–The associated numeric value is **3**. • **mschapv2**–The associated numeric value is **4**.
exp-inner-eap • Uses the expanded inner EAP authentication method. • The associated numeric value is **4**.	Use the exp-inner-eap authentication value.
credential • Uses credential authentication. • The associated numeric value is **5**.	The following authentication values apply: • **sim**– The associated numeric value is **1**. • **usim**– The associated numeric value is **2**. • **nfc-secure**– The associated numeric value is **3**. • **hw-token**– The associated numeric value is **4**. • **softoken**– The associated numeric value is **5**. • **certificate**– The associated numeric value is **6**. • **uname-password**–The associated numeric value is **7**. • **none**–The associated numeric value is **8**. • **reserved**–The associated numeric value is **9**. • **vendor-specific**–The associated numeric value is **10**.

Configuring a Venue Name Profile

You configure a venue name profile to send venue information as an ANQP IE in a GAS query response. To configure a venue name profile, enter the following commands at the command prompt:

```
(Instant AP)(config)# hotspot anqp-venue-name-profile <name>
(Instant AP)(venue-name <name>)# venue-name <name>
(Instant AP)(venue-name <name>)# venue-group <group-name>
(Instant AP)(venue-name <name>)# venue-type <type>
(Instant AP)(venue-name <name>)# venue-lang-code <language>
(Instant AP)(venue-name <name>)# enable
(Instant AP)(venue-name <name>)# end
(Instant AP)# commit apply
```

You can specify any of the following venue groups and the corresponding venue types:

Table 68: *Venue Types*

Venue Group	Associated Venue Type Value
unspecified The associated numeric value is **0**.	
assembly The associated numeric value is **1**.	• unspecified–The associated numeric value is **0**. • arena–The associated numeric value is **1**. • stadium–The associated numeric value is **2**. • passenger-terminal–The associated numeric value is **3**. • amphitheater–The associated numeric value is **4**. • amusement-park–The associated numeric value is **5**. • place-of-worship–The associated numeric value is **6**. • convention-center–The associated numeric value is **7**. • library–The associated numeric value is **8**. • museum–The associated numeric value is **9**. • restaurant–The associated numeric value is **10**. • theater–The associated numeric value is **11**. • bar –The associated numeric value is **12**. • coffee-shop –The associated numeric value is **13**. • zoo-or-aquarium –The associated numeric value is **14**. • emergency-cord-center–The associated numeric value is **15**.
business The associated numeric value is **2**.	• unspecified–The associated numeric value is **0**. • doctor–The associated numeric value is **1** • bank–The associated numeric value is **2** • fire-station–The associated numeric value is **3** • police-station–The associated numeric value is **4** • post-office–The associated numeric value is **6** • professional-office–The associated numeric value is **7** • research-and-dev-facility–The associated numeric value is **8** • attorney-office–The associated numeric value is **9**
educational The associated numeric value is **3**.	• unspecified–The associated numeric value is **0**. • school-primary–The associated numeric value is **1**. • school-secondary–The associated numeric value is **2**. • univ-or-college–The associated numeric value is **3**.
factory-and-industrial The associated numeric value is **4**.	• unspecified–The associated numeric value is **0**. • factory–The associated numeric value is **1**.
institutional	• unspecified–The associated numeric value is **0**. • hospital–The associated numeric value is **1**.

Venue Group	Associated Venue Type Value
The associated numeric value is **5**.	• long-term-care–The associated numeric value is **2**. • alc-drug-rehab–The associated numeric value is **3**. • group-home–The associated numeric value is **4**. • prison-or-jail–The associated numeric value is **5**.
mercantile The associated numeric value is **6**.	• unspecified–The associated numeric value is **0**. • retail-store–The associated numeric value is **1**. • grocery-market–The associated numeric value is **2**. • auto-service-station–The associated numeric value is **3**. • shopping-mall–The associated numeric value is **4**. • gas-station–The associated numeric value is **5**
residential The associated numeric value is **7**.	• unspecified–The associated numeric value is **0**. • private-residence–The associated numeric value is **1**. • hotel–The associated numeric value is **3** • dormitory–The associated numeric value is **4** • boarding-house–The associated numeric value is **5**.
storage The associated numeric value is **8**.	unspecified–The associated numeric value is **0**.
utility-misc The associated numeric value is **9**.	unspecified–The associated numeric value is **0**.
vehicular The associated numeric value is **10**	• unspecified–The associated numeric value is **0**. • automobile-or-truck–The associated numeric value is **1**. • airplane–The associated numeric value is **2**. • bus–The associated numeric value is **3**. • ferry–The associated numeric value is **4**. • ship –The associated numeric value is **5**. • train –The associated numeric value is **6**. • motor-bike–The associated numeric value is **7**.
outdoor The associated numeric value is **11**.	• unspecified–The associated numeric value is **0** • muni-mesh-network–The associated numeric value is **1**. • city-park–The associated numeric value is **2**. • rest-area–The associated numeric value is **3**. • traffic-control–The associated numeric value is **4** • bus-stop–The associated numeric value is **5** • kiosk –The associated numeric value is **6**

Configuring a Network Authentication Profile

You can configure a network authentication profile to define the authentication type used by the hotspot network. To configure a network authentication profile, enter the following commands at the command prompt:

```
(Instant AP)(config)# hotspot anqp-nwk-auth-profile <name>
(Instant AP)(network-auth <name>)# nwk-auth-type <type>
(Instant AP)(network-auth <name>)# url <URL>
(Instant AP)(network-auth <name>)# enable
(Instant AP)(network-auth <name>)# end
(Instant AP)# commit apply
```

You can specify any of the following network authentication type for the **nwk-auth-type <type>** command:

- **accept-term-and-cond**–When configured, the network requires the user to accept terms and conditions. This option requires you to specify a redirection URL string as an IP address, FQDN or URL.
- **online-enrollment**–When configured, the network supports the online enrollment.

- **http-redirect**–When configured, additional information on the network is provided through HTTP/HTTPS redirection.
- **dns-redirect**–When configured, additional information on the network is provided through DNS redirection. This option requires you to specify a redirection URL string as an IP address, FQDN, or URL.

Configuring a Roaming Consortium Profile

You can configure a roaming consortium profile to send the roaming consortium information as an ANQP IE in a GAS query response. To configure a roaming consortium profile, enter the following commands at the command prompt:

```
(Instant AP)(config)# hotspot anqp-roam-cons-profile <name>
(Instant AP)(roaming-consortium <name>)# roam-cons-oi <roam-cons-oi>
(Instant AP)(roaming-consortium <name>)# roam-cons-oi-len <roam-cons-oi-len>
(Instant AP)(roaming-consortium <name>)# enable
(Instant AP)(roaming-consortium <name>)# end
(Instant AP)# commit apply
```

Specify a hexadecimal string of 3 to 5 octets for **roam-cons-oi <roam-cons-oi>**.

Based on the OI specified, you can specify the following parameters for the length of OI in **roam-cons-oi-len <roam-cons-oi-len>**.

- For 0: 0 Octets in the OI (Null)
- For 3: OI length is 24-bit (3 Octets)
- For 5: OI length is 36-bit (5 Octets)

Configuring a 3GPP Profile

You can configure a 3rd Generation Partnership Project (3GPP) profile to define information for the 3G Cellular Network for hotspots.

To configure a 3GPP profile, enter the following commands at the command prompt:

```
(Instant AP)(config)# hotspot anqp-3gpp-profile <name>
(Instant AP)(3gpp <name>)# 3gpp-plmn1 <plmn-ID>
(Instant AP)(3gpp <name>)# enable
(Instant AP)(3gpp <name>)# end
(Instant AP)# commit apply
```

The Public Land Mobile Network (PLMN) ID is a combination of the mobile country code and network code. You can specify up to 6 PLMN IDs for a 3GPP profile.

Configuring an IP Address Availability Profile

You can configure the available IP address types to send information on IP address availability as an ANQP IE in a GAS query response. To configure an IP address availability profile, enter the following commands at the command prompt:

```
(Instant AP)(config)# hotspot anqp-ip-addr-avail-profile <name>
(Instant AP)(IP-addr-avail <name>)# ipv4-addr-avail
(Instant AP)(IP-addr-avail <name>)# ipv6-addr-avail
(Instant AP)(IP-addr-avail <name>)# enable
(Instant AP)(IP-addr-avail <name>)# end
(Instant AP)# commit apply
```

Configuring a Domain Profile

You can configure a domain profile to send the domain names as an ANQP IE in a GAS query response. To configure a domain name profile, enter the following commands at the command prompt:

```
(Instant AP)(config)# hotspot anqp-domain-name-profile <name>
(Instant AP)(domain-name <name>)# domain-name <domain-name>
(Instant AP)(domain-name <name>)# enable
```

```
(Instant AP)(domain-name <name>)# end
(Instant AP)# commit apply
```

Configuring an Operator-friendly Profile

You can configure the operator-friendly name profile to define the identify the operator. To configure an H2QP operator-friendly name profile:

```
(Instant AP)(config)# hotspot h2qp-oper-name-profile <name>
(Instant AP)(operator-friendly-name <name>)# op-fr-name <op-fr-name>
(Instant AP)(operator-friendly-name <name>)# op-lang-code <op-lang-code>
(Instant AP)(operator-friendly-name <name>)# enable
(Instant AP)(operator-friendly-name <name>)# end
(Instant AP)# commit apply
```

Configuring a Connection Capability Profile

You can configure a Connection Capability profile to define information such as the hotspot IP protocols and associated port numbers that are available for communication. To configure an H2QP connection capability profile:

```
(Instant AP)(config) # hotspot h2qp-conn-cap-profile
(Instant AP)(connection-capabilities <name>)# esp-port
(Instant AP)(connection-capabilities <name>)# icmp
(Instant AP)(connection-capabilities <name>)# tcp-ftp
(Instant AP)(connection-capabilities <name>)# tcp-http
(Instant AP)(connection-capabilities <name>)# tcp-pptp-vpn
(Instant AP)(connection-capabilities <name>)# tcp-ssh
(Instant AP)(connection-capabilities <name>)# tcp-tls-vpn
(Instant AP)(connection-capabilities <name>)# tcp-voip
(Instant AP)(connection-capabilities <name>)# udp-ike2
(Instant AP)(connection-capabilities <name>)# udp-ipsec-vpn
(Instant AP)(connection-capabilities <name>)# udp-voip
(Instant AP)(connection-capabilities <name>)# enable
(Instant AP)(connection-capabilities <name>)# end
(Instant AP)# commit apply
```

Configuring an Operating Class Profile

You can configure an operating class profile to list the channels on which the hotspot is capable of operating. To configure an H2QP operating class profile:

```
(Instant AP)(config) # hotspot h2qp-oper-class-profile <name>
(Instant AP)(operator-class <name>)# op-class <class-ID>
(Instant AP)(operator-class <name>)# enable
(Instant AP)(operator-class <name>)# end
(Instant AP)# commit apply
```

Configuring a WAN Metrics Profile

You can configure a WAN metrics profile to define information about access network characteristics such as link status and metrics. To configure a WAN metrics profile:

```
(Instant AP)(config)# hotspot h2qp-wan-metrics-profile <name>
(Instant AP)(WAN-metrics <name>)# at-capacity
(Instant AP)(WAN-metrics <name>)# downlink-load <load>
(Instant AP)(WAN-metrics <name>)# downlink-speed <speed>
(Instant AP)(WAN-metrics <name>)# load-duration <duration>
(Instant AP)(WAN-metrics <name>)# symm-link
(Instant AP)(WAN-metrics <name>)# uplink-load <load>
(Instant AP)(WAN-metrics <name>)# uplink-speed <speed>
(Instant AP)(WAN-metrics <name>)# wan-metrics-link-status <status>
(Instant AP)(WAN-metrics <name>)# end
(Instant AP)# commit apply
```

You can specify the following WAN downlink and uplink parameters:

- **Downlink load**– Indicates the percentage of the WAN downlink currently utilized. The default value of 0 indicates that the downlink speed is unknown or unspecified.
- **Downlink speed** –Indicates the WAN downlink speed in Kbps.
- **Uplink load**–Indicates the percentage of the WAN uplink currently utilized. The default value of 0 indicates that the downlink speed is unknown or unspecified.
- **Uplink speed**–Indicates the WAN uplink speed in Kbps.
- **Load duration**–Indicates the duration in seconds during which the downlink utilization is measured.
- **Symmetric links**–Indicates if the uplink and downlink have the same speed.
- **WAN Link Status**– Indicates if the WAN is down (link-down), up (link-up), or in test state (link-under-test).

Creating a Hotspot Profile

To create a hotspot profile:

```
(Instant AP)(config)# hotspot hs-profile <name>
(Instant AP)(Hotspot2.0 <name>)# asra
(Instant AP)(Hotspot2.0 <name>)# access-network-type <type>
(Instant AP)(Hotspot2.0 <name>)# addtl-roam-cons-ois <roam-consortium-OIs>
(Instant AP)(Hotspot2.0 <name>)# comeback-mode
(Instant AP)(Hotspot2.0 <name>)# gas-comeback <delay-interval>
(Instant AP)(Hotspot2.0 <name>)# group-frame-block
(Instant AP)(Hotspot2.0 <name>)# hessid <hotspot-essid>
(Instant AP)(Hotspot2.0 <name>)# internet
(Instant AP)(Hotspot2.0 <name>)# p2p-cross-connect
(Instant AP)(Hotspot2.0 <name>)# p2p-dev-mgmt
(Instant AP)(Hotspot2.0 <name>)# pame-bi
(Instant AP)(Hotspot2.0 <name>)# query-response-length-limit <integer>
(Instant AP)(Hotspot2.0 <name>)# roam-cons-len-1 <integer>
(Instant AP)(Hotspot2.0 <name>)# roam-cons-len-2 <integer>
(Instant AP)(Hotspot2.0 <name>)# roam-cons-len-3 <integer>
(Instant AP)(Hotspot2.0 <name>)# roam-cons-oi-1 <integer>
(Instant AP)(Hotspot2.0 <name>)# roam-cons-oi-2 <integer>
(Instant AP)(Hotspot2.0 <name>)# roam-cons-oi-3 <integer>
(Instant AP)(Hotspot2.0 <name>)# venue-group <group>
(Instant AP)(Hotspot2.0 <name>)# venue-type <type>
(Instant AP)(Hotspot2.0 <name>)# enable
(Instant AP)(Hotspot2.0 <name>)# end
(Instant AP)#commit apply
```

The hotspot profile configuration parameters are described in the following table:

Table 69: *Hotspot Configuration Parameters*

Parameter	Description
access-network-type <type>	Specify any of the following 802.11u network types. • **private** – This network is accessible for authorized users only. For example, home networks or enterprise networks that require user authentication. The corresponding integer value for this network type is 0. • **private-with-guest** – This network is accessible to guest users based on guest authentication methods. For example, enterprise networks that allow guest users with captive portal authentication. The corresponding integer value for this network type is 1. • **chargeable-public** – This network provides access to the Internet based on payment. For example, a subscription-based Internet access in a coffee shop or a hotel offering chargeable in-room Internet access service. The corresponding integer value for this network type is 2. • **free-public** –This network is accessible to all without any charges applied. For example, a hotspot in airport or other public places that provide Internet access with no additional cost. The corresponding integer value for this network type is 3. • **personal-device** – This network is accessible for personal devices. For example, a laptop or camera configured with a printer for the purpose of printing. The corresponding integer value for this network type is 4. • **emergency-services** –This network is limited to accessing emergency services only. The corresponding integer value for this network type is 5. • **test** – This network is used for test purposes only. The corresponding integer value for this network type is 14. • **wildcard** –This network indicates a wildcard network. The corresponding integer value for this network type is 15.
addtl-roam-cons-ois	Specify the number of additional roaming consortium Organization Identifiers (OIs) advertised by the AP. You can specify up to three additional OIs.
asra	Enable the Additional Steps Required for Access (asra) to indicate if additional steps are required for authentication. When enabled, the following information is sent to the client in response to an ANQP query. For ASRA, ensure that the network authentication type is associated.
comeback-mode	Enable this parameter to allow the client to obtain a GAS Request and Response as a Comeback-Request and Comeback-Response. By default, this comeback mode is disabled.
gas-comeback-delay	Specify a GAS come back delay interval in milliseconds to allow the client to retrieve the query response using a comeback request action frame when the GAS response is delayed. You can specify a value within the range of 100-2000 milliseconds and the default value is 500 milliseconds.
group-frame-block	Enable this parameter if you want to stop the AP from sending forward downstream group-addressed frames.
hessid	Specify a Homogenous Extended Service Set Identifier (HESSID) in a hexadecimal format separated by colons.
internet	Specify this parameter to allow the W-IAP to send an Information Element (IE) indicating that the network allows Internet access.
p2p-cross-connect	Specify this parameter to advertise support for P2P Cross Connections.
p2p-dev-mgmt	Specify this parameter to advertise support for P2P device management.
pame-bi	Specify this parameter to enable Pre-Association Message Exchange BSSID Independent (PAME-BI) bit, with which the W-IAP can indicate that the Advertisement Server can return a query response independent of the BSSID used in the GAS Frame exchange.

Table 69: *Hotspot Configuration Parameters*

Parameter	Description
`query-response-length-limit`	Specify this parameter to set the maximum length of the GAS query response, in octets. You can specify a value within the range of 1-127. The default value is 127.

`roam-cons-len-1`
`roam-cons-len-2`
`roam-cons-len-3`
	Specify the length of the organization identifier. The value of the **roam-cons-len-1**, **roam-cons-len-2**, or **roam-cons-len-3**. The roaming consortium OI is based on the following parameters:
	• **0**: Zero Octets in the OI (Null)
	• **3**: OI length is 24-bit (3 Octets)
	• **5**: OI length is 36-bit (5 Octets)

`venue-group`	Specify one of the following venue groups • assembly • business • educational • factory-and-industrial • institutional • mercantile • outdoor • residential • storage • utility-and-misc • vehicular By default, the business venue group is used.
`venue-type`	Specify a venue type to be advertised in the ANQP IEs from W-IAPs associated with this hotspot profile. For more information about the supported venue types for each venue group, see Table 68.

Associating an Advertisement Profile to a Hotspot Profile

To associate a hotspot profile with an advertisement profile:

```
(Instant AP)(config)# hotspot hs-profile <name>
(Instant AP)(Hotspot2.0 <name>)# advertisement-protocol <protocol>
(Instant AP)(Hotspot2.0 <name>)# advertisement-profile anqp-3gpp <name>
(Instant AP)(Hotspot2.0 <name>)# advertisement-profile anqp-domain-name <name>
(Instant AP)(Hotspot2.0 <name>)# advertisement-profile anqp-ip-addr-avail <name>
(Instant AP)(Hotspot2.0 <name>)# advertisement-profile anqp-nai-realm <name>
(Instant AP)(Hotspot2.0 <name>)# advertisement-profile anqp-nwk-auth <name>
(Instant AP)(Hotspot2.0 <name>)# advertisement-profile anqp-roam-cons <name>
(Instant AP)(Hotspot2.0 <name>)# advertisement-profile anqp-venue-name <name>
(Instant AP)(Hotspot2.0 <name>)# advertisement-profile h2qp-conn-cap <name>
(Instant AP)(Hotspot2.0 <name>)# advertisement-profile h2qp-oper-class <name>
(Instant AP)(Hotspot2.0 <name>)# advertisement-profile h2qp-oper-name <name>
(Instant AP)(Hotspot2.0 <name>)# advertisement-profile h2qp-wan-metrics <name>
(Instant AP)(Hotspot2.0 <name>)# end
(Instant AP)# commit apply
```

The configuration parameters for associating an advertisement profile with a hotspot profile are described in the following table:

Table 70: *Advertisement Association Parameters*

Parameter	Description
`advertisement-profile`	Specify the advertisement profile to associate with this hotspot profile. For information on advertisement profiles, see Creating Advertisement Profiles for Hotspot Configuration on page 340.
`advertisement-protocol`	Specify the advertisement protocol types as Access Network Query Protocol (ANQP) as **anqp**.

Creating a WLAN SSID and Associating Hotspot Profile

To create a WLAN SSID with Enterprise Security and WPA2 Encryption Settings:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name># essid <ESSID-name>
(Instant AP)(SSID Profile <name># type {<Employee> | <Voice>| <Guest>}
(Instant AP)(SSID Profile <name># vlan <vlan-ID>
(Instant AP)(SSID Profile <name># set-vlan <attribute>{equals|not-equals|starts-with|ends-
with|contains} <operator> <VLAN-ID>| value-of}
(Instant AP)(SSID Profile <name># opmode {wpa2-aes|wpa-tkip,wpa2-aes}
(Instant AP)(SSID Profile <name># blacklist
(Instant AP)(SSID Profile <name># mac-authentication
(Instant AP)(SSID Profile <name># l2-auth-failthrough
(Instant AP)(SSID Profile <name># termination
(Instant AP)(SSID Profile <name># external-server
(Instant AP)(SSID Profile <name># auth-server <server-name>
(Instant AP)(SSID Profile <name># server-load-balancing
(Instant AP)(SSID Profile <name># radius-accounting
(Instant AP)(SSID Profile <name># radius-accounting-mode {user-authentication| user-
association}
(Instant AP)(SSID Profile <name># radius-interim-accounting-interval <minutes>
(Instant AP)(SSID Profile <name># radius-reauth-interval <minutes>
(Instant AP)(SSID Profile <name># set-role-by-ssid
(Instant AP)(SSID Profile <name>)# hotspot-profile <name>
(Instant AP)(SSID Profile <name># end
(Instant AP)# commit apply
```

Sample Configuration

Step 1 - Creating ANQP and H2QP Advertisement Profile

```
(Instant AP)# configure terminal
(Instant AP)(config)# hotspot anqp-nai-realm-profile nr1
(Instant AP)(nai-realm "nr1")# nai-realm-name name1
(Instant AP)(nai-realm "nr1")# nai-realm-encoding utf8
(Instant AP)(nai-realm "nr1")# nai-realm-eap-method eap-sim
(Instant AP)(nai-realm "nr1")# nai-realm-auth-id-1 non-eap-inner-auth
(Instant AP)(nai-realm "nr1")# nai-realm-auth-value-1 mschapv2
(Instant AP)(nai-realm "nr1")# nai-home-realm
(Instant AP)(nai-realm "nr1")# exit

(Instant AP)(config)# hotspot anqp-venue-name-profile vn1
(Instant AP)(venue-name "vn1")# venue-group business
(Instant AP)(venue-name "vn1")# venue-type research-and-dev-facility
(Instant AP)(venue-name "vn1")# venue-lang-code eng
(Instant AP)(venue-name "vn1")# venue-name VenueName
(Instant AP)(venue-name "vn1")# exit

(Instant AP)(config)# hotspot anqp-nwk-auth-profile na1
```

```
(Instant AP)(network-auth "na1")# nwk-auth-type accept-term-and-cond
(Instant AP)(network-auth "na1")# url www.nwkauth.com
(Instant AP)(network-auth "na1")# exit

(Instant AP)(config)# hotspot anqp-roam-cons-profile rc1
(Instant AP)(roaming-consortium "rc1")# roam-cons-oi-len 3
(Instant AP)(roaming-consortium "rc1")# roam-cons-oi 888888
(Instant AP)(roaming-consortium "rc1")# exit

(Instant AP)(config)# hotspot anqp-3gpp-profile 3g
(Instant AP)(3gpp "3g")# 3gpp-plmn1 40486
(Instant AP)(3gpp "3g")# exit

(Instant AP)(config)# hotspot anqp-ip-addr-avail-profile ip1
(Instant AP)(IP-addr-avail "ip1")# no ipv4-addr-avail
(Instant AP)(IP-addr-avail "ip1")# ipv6-addr-avail
(Instant AP)(IP-addr-avail "ip1")# exit

(Instant AP)(config)# hotspot anqp-domain-name-profile dn1
(Instant AP)(domain-name "dn1")# domain-name DomainName
(Instant AP)(domain-name "dn1")# exit

(Instant AP)(config)# hotspot h2qp-oper-name-profile on1
(Instant AP)(operator-friendly-name"on1")# op-lang-code eng
(Instant AP) operator-friendly-name"on1")# op-fr-name OperatorFriendlyName
(Instant AP) (operator-friendly-name"on1")# exit
```

Step 2: Creating a hotspot profile

```
(Instant AP)# configure terminal
(Instant AP)(config)# hotspot hs-profile hs1
(Instant AP)(Hotspot2.0 "hs1")# enable
(Instant AP)(Hotspot2.0 "hs1")# comeback-mode
(Instant AP)(Hotspot2.0 "hs1")# gas-comeback-delay 10
(Instant AP)(Hotspot2.0 "hs1")# no asra
(Instant AP)(Hotspot2.0 "hs1")# no internet
(Instant AP)(Hotspot2.0 "hs1")# query-response-length-limit 20
(Instant AP)(Hotspot2.0 "hs1")# access-network-type chargeable-public
(Instant AP)(Hotspot2.0 "hs1")# roam-cons-len-1 3
(Instant AP)(Hotspot2.0 "hs1")# roam-cons-oi-1 123456
(Instant AP)(Hotspot2.0 "hs1")# roam-cons-len-2 3
(Instant AP)(Hotspot2.0 "hs1")# roam-cons-oi-2 223355
(Instant AP)(Hotspot2.0 "hs1")# addtl-roam-cons-ois 0
(Instant AP)(Hotspot2.0 "hs1")# venue-group business
(Instant AP)(Hotspot2.0 "hs1")# venue-type research-and-dev-facility
(Instant AP)(Hotspot2.0 "hs1")# pame-bi
(Instant AP)(Hotspot2.0 "hs1")# group-frame-block
(Instant AP)(Hotspot2.0 "hs1")# p2p-dev-mgmt
(Instant AP)(Hotspot2.0 "hs1")# p2p-cross-connect
(Instant AP)(Hotspot2.0 "hs1")# end
(Instant AP)# commit apply
```

Step 3: Associating advertisement profiles with the hotspot profile

```
(Instant AP)# configure terminal
(Instant AP)(config)# hotspot hs-profile hs1
(Instant AP)(Hotspot2.0 "hs1")# advertisement-profile anqp-nai-realm nr1
(Instant AP)(Hotspot2.0 "hs1")# advertisement-profile anqp-venue-name vn1
(Instant AP)(Hotspot2.0 "hs1")# advertisement-profile anqp-nwk-auth na1
(Instant AP)(Hotspot2.0 "hs1")# advertisement-profile anqp-roam-cons rc1
(Instant AP)(Hotspot2.0 "hs1")# advertisement-profile anqp-3gpp 3g1
(Instant AP)(Hotspot2.0 "hs1")# advertisement-profile anqp-ip-addr-avail ip1
(Instant AP)(Hotspot2.0 "hs1")# advertisement-profile anqp-domain-name dn1
(Instant AP)(Hotspot2.0 "hs1")# advertisement-profile h2qp-oper-name on1
```

```
(Instant AP)(Hotspot2.0 "hs1")# advertisement-profile h2qp-wan-metrics wm1
(Instant AP)(Hotspot2.0 "hs1")# advertisement-profile h2qp-conn-cap cc1
(Instant AP)(Hotspot2.0 "hs1")# advertisement-profile h2qp-oper-class oc1
(Instant AP)(Hotspot2.0 "hs1")# exit
```

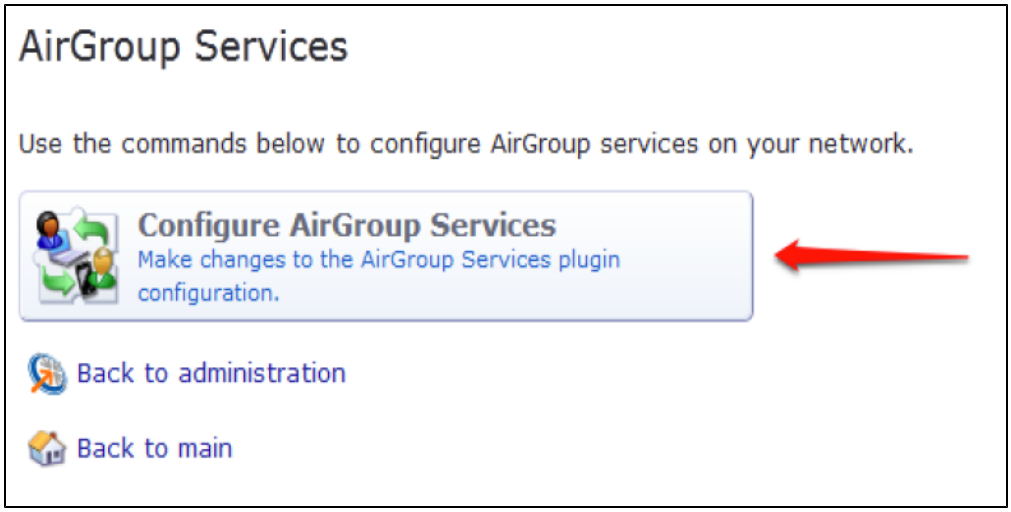
Step 4: Associate the hotspot profile with WLAN SSID:

```
(Instant AP)# configure terminal
(Instant AP)# wlan ssid-profile ssidProfile1
(Instant AP)(SSID Profile "ssidProfile1")# essid hsProf
(Instant AP)(SSID Profile "ssidProfile1")# type employee
(Instant AP)(SSID Profile "ssidProfile1")# vlan 200
(Instant AP)(SSID Profile "ssidProfile1")# opmode wpa2-aes
(Instant AP)(SSID Profile "ssidProfile1")# blacklist
(Instant AP)(SSID Profile "ssidProfile1")# mac-authentication
(Instant AP)(SSID Profile "ssidProfile1")# l2-auth-failthrough
(Instant AP)(SSID Profile "ssidProfile1")# radius-accounting
(Instant AP)(SSID Profile "ssidProfile1")# radius-accounting-mode user-association
(Instant AP)(SSID Profile "ssidProfile1")# radius-interim-accounting-interval 10
(Instant AP)(SSID Profile "ssidProfile1")# radius-reauth-interval 20
(Instant AP)(SSID Profile "ssidProfile1")# max-authentication-failures 2
(Instant AP)(SSID Profile "ssidProfile1")# set-role-by-ssid
(Instant AP)(SSID Profile "ssidProfile1")# hotspot-profile hs1
(Instant AP)(SSID Profile "ssidProfile1")# end
(Instant AP)# commit apply
```

To configure ClearPass Guest:

1. On ClearPass Guest, navigate to **Administration > AirGroup Services**.
2. Click **Configure AirGroup Services**.

Figure 128 *Configure AirGroup Services*


AirGroup Services
Use the commands below to configure AirGroup services on your network.
Configure AirGroup Services
Make changes to the AirGroup Services plugin configuration.
Back to administration
Back to main

3. Click **Add a new controller**.
4. Update the fields with the appropriate information.

NOTE

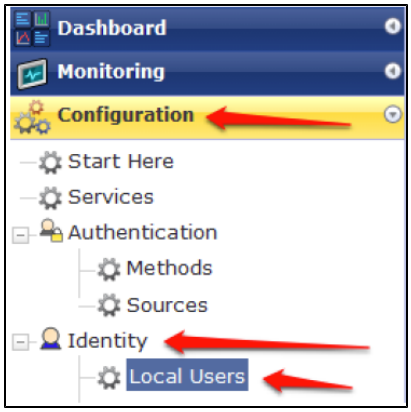
Ensure that the port configured matches the CoA port (RFC 3576) set on the W-IAP configuration.

5. Click **Save Configuration**.

In order to demonstrate AirGroup, either an AirGroup Administrator or an AirGroup Operator account must be created.

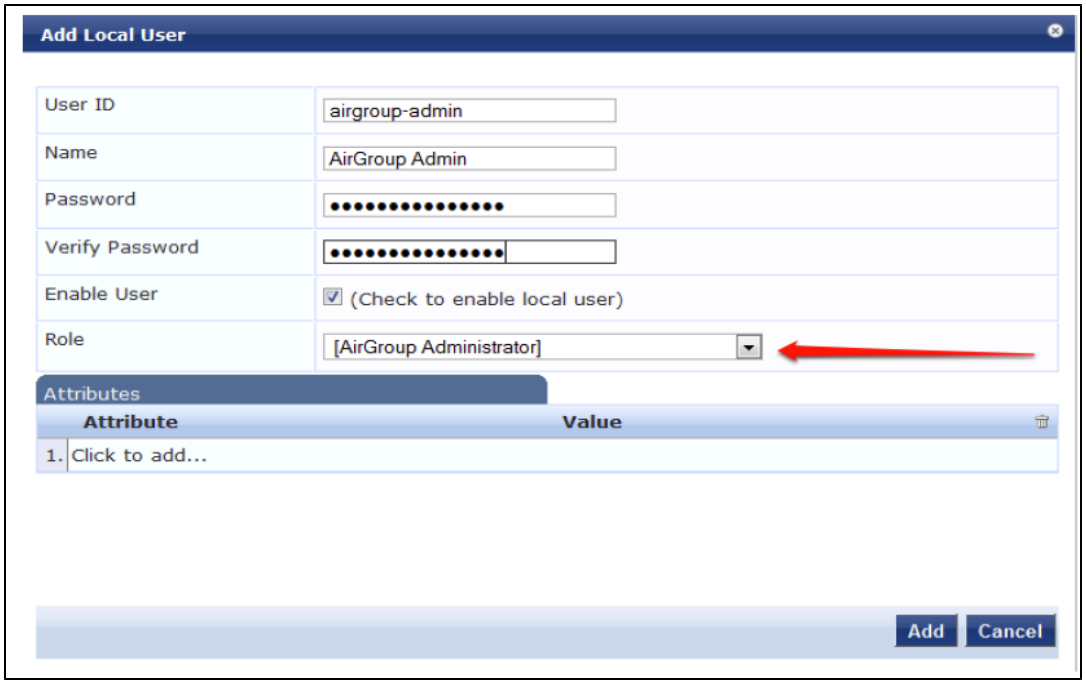
1. Navigate to the ClearPass Policy Manager UI, and navigate to **Configuration > Identity > Local Users**.

Figure 129 *Configuration > Identity > Local Users Selection*



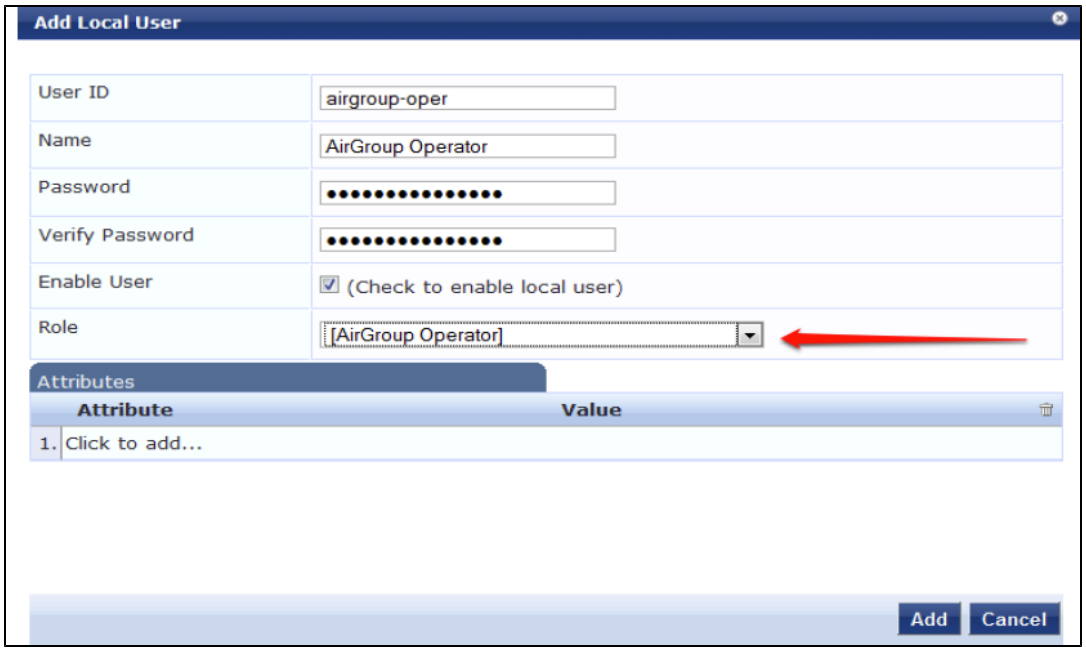
2. Click **Add User**.
3. Create an **AirGroup Administrator**.

Figure 130 *Create an AirGroup Administrator*



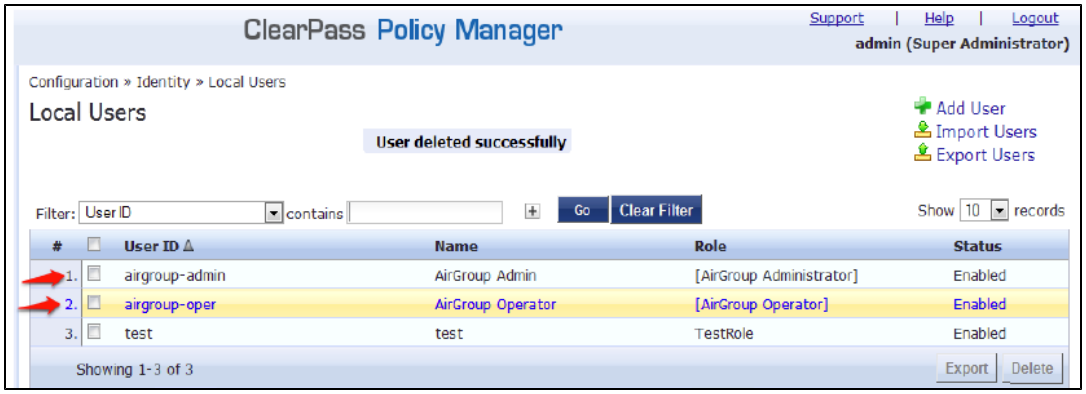
4. In this example, the password used is test123. Click **Add**.
5. Now click **Add User**, and create an **AirGroup Operator**.

Figure 131 *Create an AirGroup Operator*



6. Click **Add** to save the user with an **AirGroup Operator** role. The **AirGroup Administrator** and **AirGroup Operator IDs** will be displayed in the **Local Users UI** screen.

Figure 132 *Local Users UI Screen*


ClearPass Policy Manager
Support | Help | Logout
admin (Super Administrator)
Configuration » Identity » Local Users
Local Users
User deleted successfully
Add User
Import Users
Export Users
Filter: User ID contains Go Clear Filter Show 10 records
User ID Name Role Status
1. airgroup-admin AirGroup Admin [AirGroup Administrator] Enabled
2. airgroup-oper AirGroup Operator [AirGroup Operator] Enabled
3. test test TestRole Enabled
Showing 1-3 of 3
Export Delete

7. Navigate to the ClearPass Guest UI and click **Logout**. The **ClearPass Guest Login** page is displayed. Use the AirGroup admin credentials to log in.
8. After logging in, click **Create Device**.

Figure 133 *Create a Device*

The following page is displayed.

Figure 134 *- Register Shared Device*

Register Shared Device
* Device Name:
Enter a name to identify the device.
* MAC Address:
Enter the MAC address of the device.
Shared Locations:
Enter a list of location IDs where this device will be shared.
Use a comma-separated list of tag=value pairs; tag may be AP-Name, AP-Group, or FQLN.
A fully qualified location name is '<ap-name>.floor<N>.<building-name>.<campus>'.
Leave blank to share with all locations.
Shared With:
Enter up to 10 usernames that will be able to use this device.
Use a comma-separated list, e.g. user1,user2,user3, or blank for all users.
Shared Roles:
List the user roles that will be able to use this device.
Use a comma-separated list, e.g. role1,role2,role3, or blank for all roles.
Register Shared Device

For this test, add your AppleTV device name and MAC address but leave all other fields empty.

9. Click **Register Shared Device**.

Testing

To verify the setup:

1. Disconnect your AppleTV and OSX Mountain Lion/iOS 6 devices if they were previously connected to the wireless network. Remove their entries from the controller's user table using these commands:
   - Find the MAC address– `show user table`
   - Delete the address from the table– `aaa user delete mac 00:aa:22:bb:33:cc`
2. Reconnect both devices. To limit access to the AppleTV, access the ClearPass Guest UI using either the AirGroup admin or the AirGroup operator credentials. Next, navigate to **List Devices > Test Apple TV > Edit**. Add a username that is not used to log in to the Apple devices in the **Shared With field**.
3. Disconnect and remove the OSX Mountain Lion/iOS 6 device from the controller's user table. Reconnect the device by not using the username that you added to the **Shared With field**. The AppleTV should not be available to this device.
4. Disconnect the OSX Mountain Lion/iOS 6 device and delete it from the controller's user table. Reconnect using the username that was added to the **Shared With field**. The OSX Mountain Lion/iOS 6 device should once again have access to the AppleTV.

Troubleshooting

Table 71: *Troubleshooting*

Problem	Solution
Limiting devices has no effect.	Ensure IPv6 is disabled.
Apple Macintosh running Mountain Lion can use AirPlay but iOS devices cannot.	Ensure IPv6 is disabled.

This section describes the most common IAP-VPN deployments models and provides information to carry out the necessary configuration procedures. The examples in this section refer to more than one DHCP profile and wired port configuration in addition to wireless SSID configuration. All these are optional. In most networks, a single DHCP profile and wireless SSID configuration referring a DHCP profile is sufficient.

The following scenarios are described in this section:

- Scenario 1 - IPSec: Single Datacenter Deployment with No Redundancy on page 357
- Scenario 2 - IPSec: Single Datacenter with Multiple Controllers for Redundancy on page 360
- Scenario 3 - IPSec: Multiple Datacenter Deployment with Primary and Backup Controllers for Redundancy on page 364
- Scenario 4 - GRE: Single Datacenter Deployment with No Redundancy on page 369

Scenario 1 - IPSec: Single Datacenter Deployment with No Redundancy

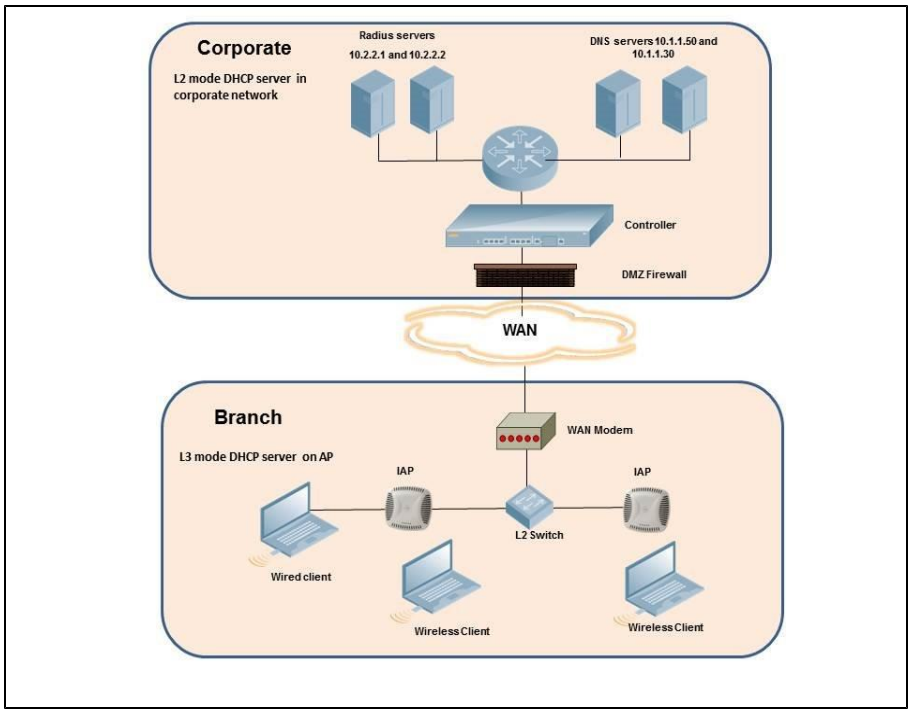
This scenario includes the following configuration elements:

1. Single VPN primary configuration using IPSec
2. Split tunneling of client traffic
3. Split tunneling of DNS traffic from clients
4. Distributed L3 and Centralized L2 mode DHCP
5. RADIUS server within corporate network and authentication survivability for branch survivability
6. Wired and wireless users in L2 and L3 modes respectively
7. Access rules defined for wired and wireless networks to permit all traffic

Topology

Figure 135 shows the topology and the IP addressing scheme used in this scenario.

Figure 135 *Scenario 1 - IPSec: Single datacenter Deployment with No Redundancy*



The following IP addresses are used in the examples for this scenario:

- 10.0.0.0/8 is the corporate network
- 10.20.0.0/16 subnet is reserved for L2 mode
- 10.30.0.0/16 subnet is reserved for L3 mode
- Client count in each branch is 200

AP Configuration

The following table provides information on the configuration steps performed through the CLI with example values. For information on the UI procedures, see the topics referenced in the *UI Navigation Details* column.

Table 72: *W-IAP Configuration for Scenario 1 - IPSec: Single Datacenter Deployment with No Redundancy*

Configuration Steps	CLI Commands	UI Procedure
1. Configure the primary host for VPN with the Public VRRP IP address of the controller.	`(ap)(config)# vpn primary <public VRRP IP of controller>`	See Configuring an IPSec Tunnel
2. Configure a routing profile to tunnel all 10.0.0.0/8 subnet traffic to controller.	`(ap)(config)# routing-profile` (ap)(routing-profile)# route 10.0.0.0 255.0.0.0 <public VRRP IP of controller>	See Configuring Routing Profiles
3. Configure Enterprise DNS for split DNS. The example in the next column uses a specific enterprise domain to only tunnel all DNS queries matching that domain to corporate.	`(ap)(config)# internal-domains` `(ap)(domains)# domain-name corpdomain.com`	See Configuring Enterprise Domains

4. Configure centralized L2 and distributed L3 with VLAN 20 and 30 respectively.	**`Centralized L2 profile`** `(ap)(config)# ip dhcp l2-dhcp`
	`(ap)(DHCP Profile "l2-dhcp")# server-type Centralized,L2`
	`(ap)(DHCP Profile "l2-dhcp")# server-vlan 20`
	`Distributed L3 profile`
	`(ap)(config)# ip dhcp l3-dhcp`
	`(ap)(DHCP Profile "l3-dhcp")# server-type Distributed,L3`
	`(ap)(DHCP Profile "l3-dhcp")# server-vlan 30`
	`(ap)(DHCP Profile "l3-dhcp")# ip-range 10.30.0.0 10.30.255.255`
	`(ap)(DHCP Profile "l3-dhcp")# dns-server 10.1.1.50,10.1.1.30`
	`(ap)(DHCP Profile "l3-dhcp")# domain-name corpdomain.com`
	`(ap)(DHCP Profile "l3-dhcp")# client-count 200`
	
	NOTE: The IP range configuration on each branch will be the same. Each W-IAP will derive a smaller subnet based on the client count scope using the Branch ID (BID) allocated by controller.
		See Configuring a Centralized DHCP Scope and Configuring Distributed DHCP Scopes

5. Create authentication servers for user authentication. The example in the next column assumes 802.1x SSID.	`(ap)(config)# wlan auth-server server1`
	`(ap)(Auth Server "server1")# ip 10.2.2.1`
	`(ap)(Auth Server "server1")# port 1812`
	`(ap)(Auth Server "server1")# acctport 1813`
	`(ap)(Auth Server "server1")# key "presharedkey"`
	`(ap)(Auth Server "server1")# exit`
	`(ap)(config)# wlan auth-server server2`
	`(ap)(Auth Server "server2")# ip 10.2.2.2`
	`(ap)(Auth Server "server2")# port 1812`
	`(ap)(Auth Server "server2")# acctport 1813`
	`(ap)(Auth Server "server2")# key "presharedkey"`
		See Configuring an External Server for Authentication

6. Configure wired and wireless SSIDs using the authentication servers and access rules created	Configure wired ports to operate in L2 mode and associate centralized L2 mode VLAN 20 to the wired port profile. `(ap)(config) # wired-port-profile wired-port`	See Configuring a Wired Profile and Wireless

Table 72: *W-IAP Configuration for Scenario 1 - IPSec: Single Datacenter Deployment with No Redundancy*

Configuration Steps	CLI Commands	UI Procedure
above and enable authentication survivability.	(ap)(wired-port-profile "wired-port")# switchport-mode access (ap)(wired-port-profile "wired-port")# allowed-vlan all (ap)(wired-port-profile "wired-port")# native-vlan 20 (ap)(wired-port-profile "wired-port")# no shutdown (ap)(wired-port-profile "wired-port")# access-rule-name wired-port (ap)(wired-port-profile "wired-port")# type employee (ap)(wired-port-profile "wired-port")# auth-server server1 (ap)(wired-port-profile "wired-port")# auth-server server2 (ap)(wired-port-profile "wired-port")# dot1x (ap)(wired-port-profile "wired-port")# exit (ap)(config)# enet1-port-profile wired-port Configure a wireless SSID to operate in L3 mode and associate distributed L3 mode VLAN 30 to the WLAN SSID profile. (ap)(config) # wlan ssid-profile wireless-ssid (ap)(SSID Profile "wireless-ssidt")# enable (ap)(SSID Profile "wireless-ssid")# type employee (ap)(SSID Profile "wireless-ssid")# essid wireless-ssid (ap)(SSID Profile "wireless-ssid")# opmode wpa2-aes (ap)(SSID Profile "wireless-ssid")# vlan 30 (ap)(SSID Profile "wireless-ssid")# auth-server server1 (ap)(SSID Profile "wireless-ssid")# auth-server server2 (ap)(SSID Profile "wireless-ssid")# auth-survivability	Network Profiles
7. Create access rule for wired and wireless authentication. In this example, the rule permits all traffic.	For wired profile: (ap)(config)# wlan access-rule wired-port (ap)(Access Rule "wired-port")# rule any any match any any any permit For WLAN SSID: (ap)(config)# wlan access-rule wireless-ssid (ap)(Access Rule "wireless-ssid")# rule any any match any any any permit	See Configuring Access Rules for Network Services
NOTE: Ensure that you execute the **commit apply** command in the Instant CLI before saving the configuration and propagating changes across the W-IAP cluster.		

AP Connected Switch Configuration

Client VLANs defined in this example must be opened on the upstream switches in multi AP deployments, as client traffic from slave to master is tagged with the client VLAN.

Datacenter Configuration

For information on controller configuration, see Configuring a Controller for IAP-VPN Operations on page 227. Ensure that the upstream router is configured with a static route pointing to the controller for the L3 VLAN.

Scenario 2 - IPSec: Single Datacenter with Multiple Controllers for Redundancy

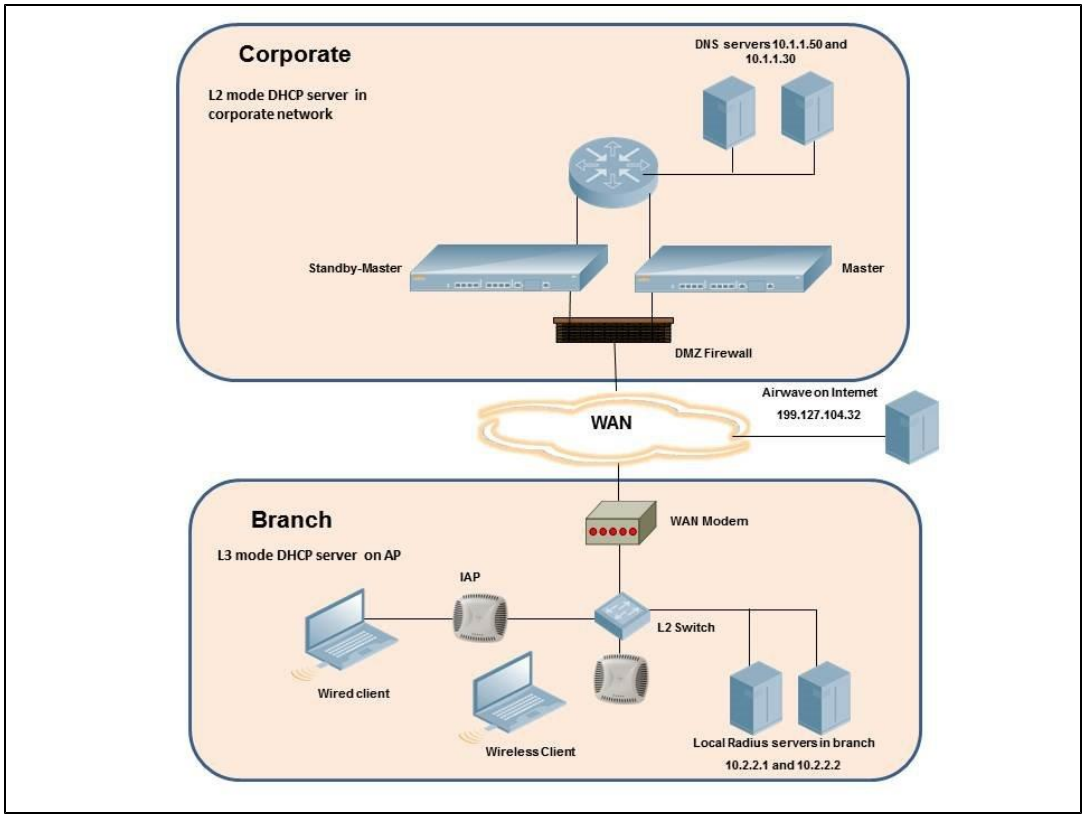
This scenario includes the following configuration elements:

- A VRRP instance between the master/standby-master pair, which is configured as the primary VPN IP address.
- Tunneling of all traffic to datacenter.
- Exception route to bypass tunneling of RADIUS and W-AirWave traffic, which are locally reachable in the branch and the Internet respectively.
- All client DNS queries are tunneled to the controller.
- Distributed L3 and Centralized L2 mode DHCP on all branches. L3 is used by the employee network and L2 is used by the guest network with captive portal.
- Wired and wireless users in L2 and L3 modes.
- Access rules defined for wired and wireless networks.

Topology

Figure 136 shows the topology and the IP addressing scheme used in this scenario.

Figure 136 *Scenario 2 - IPSec: Single Datacenter with Multiple controllers for Redundancy*



The following IP addresses are used in the examples for this scenario:

- 10.0.0.0/8 is the corporate network
- 10.20.0.0/16 subnet is reserved for L2 mode – used for guest network
- 10.30.0.0/16 subnet is reserved for L3 mode
- Client count in each branch is 200

- 10.2.2.0/24 is a branch owned subnet, which needs to override global routing profile
- 199.127.104.32 is used an example IP address of the W-AirWave server in the Internet

AP Configuration

The following table provides information on the configuration steps performed through the CLI with example values. For information on the UI procedures, see the topics referenced in the *UI Navigation Details* column.

Table 73: *W-IAP Configuration for Scenario 2 - IPSec: Single Datacenter with Multiple controllers for Redundancy*

Configuration Steps	CLI Commands	UI Procedure
1. Configure the primary host for VPN with the Public VRRP IP address of the controller.	`(ap)(config)# vpn primary <public VRRP IP of controller>`	See Configuring an IPSec Tunnel
2. Configure routing profiles to tunnel traffic through IPSec.	`(ap)(config)# routing-profile` (ap)(routing-profile)# route 0.0.0.0 0.0.0.0 <public VRRP IP of controller>	See Configuring Routing Profiles

3. Define routing profile exception RADIUS server and W-AirWave IPs, since the design requirement for this solution requires local RADIUS authentication, even though the IP matches the routing profile destination.	`(ap)(config)# routing-profile`
	`(ap)(routing-profile)# route 10.2.2.1 255.255.255.255 0.0.0.0`
	`(ap)(routing-profile)# route 10.2.2.2 255.255.255.255 0.0.0.0`
	`(ap)(routing-profile)# route 199.127.104.32 255.255.255.255 0.0.0.0`
		See Configuring Routing Profiles

4. Configure Enterprise DNS. The configuration example in the next column tunnels all DNS queries to the original DNS server of clients without proxying on W-IAP.	`(ap)(config)# internal-domains` `(ap)(domains)# domain-name *`	See Configuring Enterprise Domains

5. Configure centralized L2 and distributed L3 with VLAN 20 and 30 respectively.	**`Centralized L2 profile`**
	`(ap)(config)# ip dhcp l2-dhcp`
	`(ap)(DHCP Profile "l2-dhcp")# server-type Centralized,L2`
	`(ap)(DHCP Profile "l2-dhcp")# server-vlan 20`
	`Distributed L3 profile`
	`(ap)(config)# ip dhcp l3-dhcp`
	`(ap)(DHCP Profile "l3-dhcp")# server-type Distributed,L3`
	`(ap)(DHCP Profile "l3-dhcp")# server-vlan 30`
	`(ap)(DHCP Profile "l3-dhcp")# ip-range 10.30.0.0 10.30.255.255`
	`(ap)(DHCP Profile "l3-dhcp")# dns-server 10.1.1.50,10.1.1.30`
	`(ap)(DHCP Profile "l3-dhcp")# domain-name corpdomain.com`
	`(ap)(DHCP Profile "l3-dhcp")# client-count 200`
		See Configuring a Centralized DHCP Scope and Configuring Distributed DHCP Scopes

Table 73: *W-IAP Configuration for Scenario 2 - IPSec: Single Datacenter with Multiple controllers for Redundancy*

Configuration Steps	CLI Commands	UI Procedure
	NOTE: The IP range configuration on each branch will be the same. Each W-IAP will derive a smaller subnet based on the client count scope using the Branch ID (BID) allocated by controller.	

6. Create authentication servers for user authentication. The example in the next column assumes 802.1x SSID.	`(ap)(config)# wlan auth-server server1`
	`(ap)(Auth Server "server1")# ip 10.2.2.1`
	`(ap)(Auth Server "server1")# port 1812`
	`(ap)(Auth Server "server1")# acctport 1813`
	`(ap)(Auth Server "server1")# key "presharedkey"`
	`(ap)(Auth Server "server1")# exit`
	
	`(ap)(config)# wlan auth-server server2`
	`(ap)(Auth Server "server2")# ip 10.2.2.2`
	`(ap)(Auth Server "server2")# port 1812`
	`(ap)(Auth Server "server2")# acctport 1813`
	`(ap)(Auth Server "server2")# key "presharedkey"`
		See Configuring an External Server for Authentication

7. Configure wired and wireless SSIDs using the authentication servers and access rules created above and enable authentication survivability.	Configure wired ports to operate in L3 mode and associate distributed L3 mode VLAN 30 to the wired port profile.
	`(ap)(config) # wired-port-profile wired-port`
	`(ap)(wired-port-profile "wired-port")# switchport-mode access`
	`(ap)(wired-port-profile "wired-port")# allowed-vlan all`
	`(ap)(wired-port-profile "wired-port")# native-vlan 30`
	`(ap)(wired-port-profile "wired-port")# no shutdown`
	`(ap)(wired-port-profile "wired-port")# access-rule-name wired-port`
	`(ap)(wired-port-profile "wired-port")# type employee`
	`(ap)(wired-port-profile "wired-port")# auth-server server1`
	`(ap)(wired-port-profile "wired-port")# auth-server server2`
	`(ap)(wired-port-profile "wired-port")# dot1x`
	`(ap)(wired-port-profile "wired-port")# exit`
	`(ap)(config)# enet1-port-profile wired-port`
	
	Configure a wireless SSID to operate in L2 mode and associate Centralized L2 mode VLAN 20 to the WLAN SSID profile.
	`(ap)(config) # wlan ssid-profile guest`
	`(ap)(SSID Profile "guest")# enable`
	`(ap)(SSID Profile "guest")# type guest`
	`(ap)(SSID Profile "guest")# essid guest`
	`(ap)(SSID Profile "guest")# opmode opensystem`
	`(ap)(SSID Profile "guest")# vlan 20`
	`(ap)(SSID Profile "guest")# auth-server server1`
	`(ap)(SSID Profile "guest")# auth-server server2`
	`(ap)(SSID Profile "guest")# captive-portal internal`
	
	NOTE: This example uses internal captive portal use case using external authentication server. You can also use an external captive portal example.
	NOTE: The SSID type **guest** is used in this example to enable configuration of captive portal. However, corporate access through VPN tunnel is still allowed for this SSID because the VLAN associated to this SSID is a VPN enabled VLAN (20 in this example).
		See Configuring a Wired Profile and Wireless Network Profiles

Table 73: *W-IAP Configuration for Scenario 2 - IPSec: Single Datacenter with Multiple controllers for Redundancy*

Configuration Steps	CLI Commands	UI Procedure
8. Create access rule for wired and wireless authentication. In this example, the rule permits all traffic.	For wired profile: (ap)(config)# wlan access-rule wired-port (ap)(Access Rule "wired-port")# rule any any match any any any permit For WLAN SSID: (ap)(config)# wlan access-rule guest (ap)(Access Rule "guest")# rule any any match any any any permit	See Configuring Access Rules for Network Services
NOTE: Ensure that you execute the **commit apply** command in the Instant CLI before saving the configuration and propagating changes across the W-IAP cluster.		

AP Connected Switch Configuration

Client VLANs defined in this example must be opened on the upstream switches in multiple AP deployments, as client traffic from slave to master is tagged with the client VLAN.

Datacenter Configuration

For information on controller configuration, see Configuring a Controller for IAP-VPN Operations on page 227. Ensure that the upstream router is configured with a static route pointing to the controller for the L3 VLAN.

Scenario 3 - IPSec: Multiple Datacenter Deployment with Primary and Backup Controllers for Redundancy

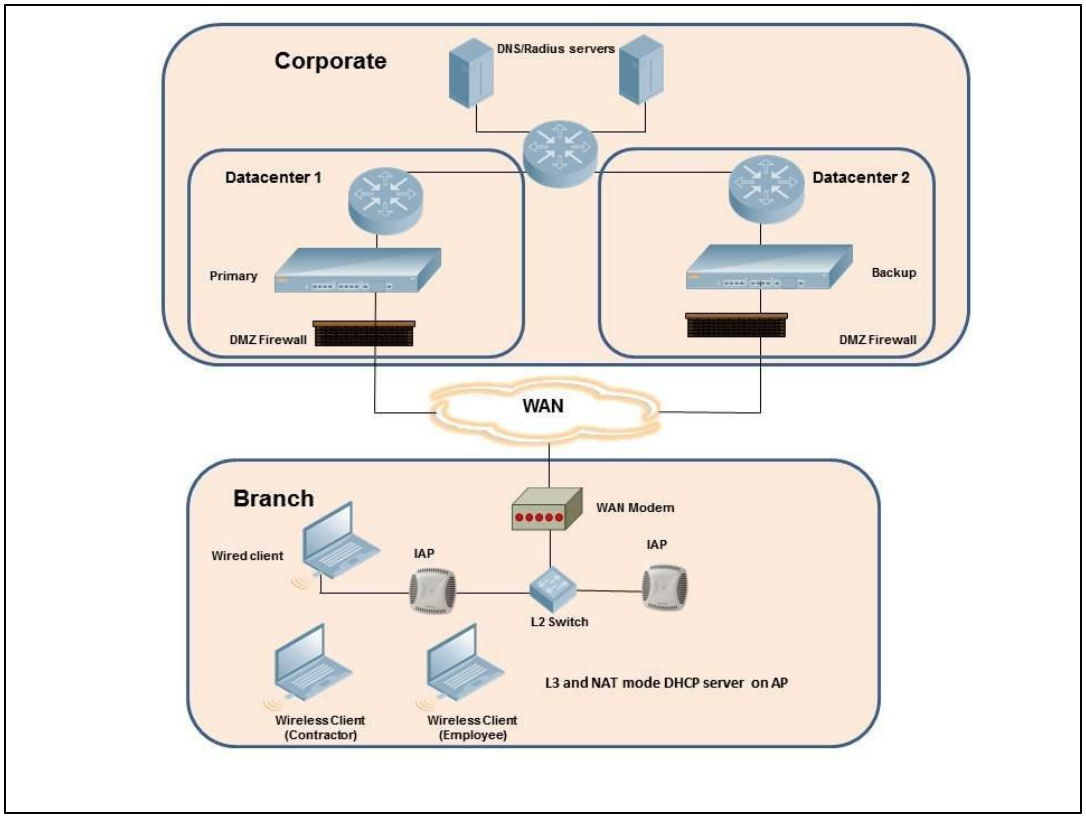
This scenario includes the following configuration elements:

- Multiple controller deployment model with controllers in different datacenters operating as primary/backup VPN with fast-failover and pre-emption enabled.
- Split tunneling of traffic.
- Split tunneling of client DNS traffic.
- Two Distributed L3 mode DHCPs, one each for employee and contractors and one Local mode DHCP server.
- RADIUS server within corporate network and authentication survivability enabled for branch survivability.
- Wired and wireless users in L3 and NAT modes respectively.
- Access rules for wired and wireless users with source NAT based rule for contractor roles to bypass global routing profile.
- OSPF based route propagation on controller.

Topology

Figure 137 shows the topology and the IP addressing scheme used in this scenario.

Figure 137 *Scenario 3 - IPSec: Multiple Datacenter Deployment with Primary and Backup Controllers for Redundancy*



The IP addressing scheme used in this example is as follows:

- 10.0.0.0/8 is the corporate network.
- 10.30.0.0/16 subnet is reserved for L3 mode -used by Employee SSID.
- 10.40.0.0/16 subnet is reserved for L3 mode -used by Contractor SSID.

- 172.16.20.0/24 subnet is used for NAT mode - used for wired network.
- Client count in each branch is 200.
- Contractors are only permitted to reach 10.16.0.0/16 network.

AP Configuration

This section provides information on configuration steps performed through the CLI or the UI.

Table 74: *W-IAP Configuration for Scenario 3 - IPSec: Multiple Datacenter Deployment*

Configuration Steps	CLI Commands	UI Procedure

1. Configure the primary IP address. This IP address is the Public IP address of the controller. Fast failover is enabled for fast convergence.	`(ap)(config)# vpn primary <public IP of primary controller>`
	`(ap)(config)# vpn backup <public IP of backup controlleres>`
	`(ap)(config)# vpn preemption`
	`(ap)(config)# vpn fast-failover`
		See Configuring an IPSec Tunnel

2. Configure routing profiles to tunnel traffic through IPSec.	`(ap)(config)# routing-profile` (ap)(routing-profile)# route 0.0.0.0 0.0.0.0 <public IP of primary controller> (ap)(routing-profile)# route 10.0.0.0 255.0.0.0 <public IP of backup controller>	See Configuring Routing Profiles
3. Configure Enterprise DNS for split DNS. The example in the next column uses a specific enterprise domain to tunnel all DNS queries matching that domain to corporate.	`(ap)(config)# internal-domains` `(ap)(domains)# domain-name corpdomain.com`	See Configuring Enterprise Domains

4. Configure distributed L3 DHCP profiles with VLAN 30 and 40.	**`Distributed L3 profile with VLAN 30`**
	`(ap)(config)# ip dhcp l3-dhcp`
	`(ap)(DHCP profile "l3-dhcp")# server-type Distributed,L3`
	`(ap)(DHCP profile "l3-dhcp")# server-vlan 30`
	`(ap)(DHCP profile "l3-dhcp")# ip-range 10.30.0.0 10.30.255.255`
	`(ap)(DHCP profile "l3-dhcp")# dns-server 10.1.1.50,10.1.1.30`
	`(ap)(DHCP profile "l3-dhcp")# domain-name corpdomain.com`
	`(ap)(DHCP profile "l3-dhcp")# client-count 200`
	`Distributed L3 profile with VLAN 40`
	`(ap)(config)# ip dhcp l3-dhcp`
	`(ap)(DHCP profile "l3-dhcp")# server-type Distributed,L3`
	`(ap)(DHCP profile "l3-dhcp")# server-vlan 40`
	`(ap)(DHCP profile "l3-dhcp")# ip-range 10.40.0.0 10.40.255.255`
	`(ap)(DHCP profile "l3-dhcp")# dns-server 10.1.1.50,10.1.1.30`
	`(ap)(DHCP profile "l3-dhcp")# domain-name corpdomain.com`
	`(ap)(DHCP profile "l3-dhcp")# client-count 200`
	Local profile with VLAN 20
		See Configuring Distributed DHCP Scopes and Configuring Local and Local,L3 DHCP Scopes

Table 74: *W-IAP Configuration for Scenario 3 - IPSec: Multiple Datacenter Deployment*

Configuration Steps	CLI Commands	UI Procedure
	(ap)(config)# ip dhcp local (ap)(DHCP profile "local")# server-type Local (ap)(DHCP profile "local")# server-vlan 20 (ap)(DHCP profile "local")# subnet 172.16.20.1 (ap)(DHCP profile "local")# subnet-mask 255.255.255.0 (ap)(DHCP profile "local")# lease-time 86400 (ap)(DHCP profile "local")# dns-server 10.1.1.30,10.1.1.50 (ap)(DHCP profile "local")# domain-name arubanetworks.com **NOTE:** The IP range configuration on each branch will be the same. Each W-IAP will derive a smaller subnet based on the client count scope using the Branch ID (BID) allocated by controller.	
5. Create authentication servers for user authentication. The example in the next column assumes 802.1x SSID.	(ap)(config)# wlan auth-server server1 (ap)(Auth Server "server1")# ip 10.2.2.1 (ap)(Auth Server "server1")# port 1812 (ap)(Auth Server "server1")# acctport 1813 (ap)(Auth Server "server1")# key "presharedkey" (ap)(Auth Server "server1")# exit (ap)(config)# wlan auth-server server2 (ap)(Auth Server "server1")# ip 10.2.2.2 (ap)(Auth Server "server1")# port 1812 (ap)(Auth Server "server1")# acctport 1813 (ap)(Auth Server "server1")# key "presharedkey"	See Configuring an External Server for Authentication
6. Configure wired and wireless SSIDs using the authentication servers and access rules and enable authentication survivability.	Configure wired ports to operate in NAT mode and associate VLAN 20 to the wired port profile. (ap)(config) # wired-port-profile wired-port (ap)(wired-port-profile "wired-port")# switchport-mode access (ap)(wired-port-profile "wired-port")# allowed-vlan all (ap)(wired-port-profile "wired-port")# native-vlan 20 (ap)(wired-port-profile "wired-port")# no shutdown (ap)(wired-port-profile "wired-port")# access-rule-name wired-port (ap)(wired-port-profile "wired-port")# type employee (ap)(wired-port-profile "wired-port")# auth-server server1 (ap)(wired-port-profile "wired-port")# auth-server server2 (ap)(wired-port-profile "wired-port")# dot1x (ap)(wired-port-profile "wired-port")# exit (ap)(config)# enet1-port-profile wired-port Configure a wireless SSID to operate in L3 mode for employee and associate distributed L3 mode VLAN 30 to the WLAN SSID profile. (ap)(config) # wlan ssid-profile wireless-ssid (ap)(SSID Profile "wireless-ssid")# enable (ap)(SSID Profile "wireless-ssid")# type employee	See Configuring a Wired Profile and Wireless Network Profiles

Table 74: *W-IAP Configuration for Scenario 3 - IPSec: Multiple Datacenter Deployment*

Configuration Steps	CLI Commands	UI Procedure
	(ap)(SSID Profile "wireless-ssid")# essid wireless-ssid (ap)(SSID Profile "wireless-ssid")# opmode wpa2-aes (ap)(SSID Profile "wireless-ssid")# vlan 30 (ap)(SSID Profile "wireless-ssid")# auth-server server1 (ap)(SSID Profile "wireless-ssid")# auth-server server2 (ap)(SSID Profile "wireless-ssid")# auth-survivability Configure a wireless SSID is configured to operate in L3 mode for contractor and associate distributed L3 mode VLAN 40 to the WLAN SSID profile. (ap)(config) # wlan ssid-profile wireless-ssid-contractor (ap)(SSID Profile "wireless-ssid-contractor")# enable (ap)(SSID Profile "wireless-ssid-contractor")# type employee (ap)(SSID Profile "wireless-ssid-contractor")# essid wireless-ssid-contractor (ap)(SSID Profile "wireless-ssid-contractor")# opmode wpa2-aes (ap)(SSID Profile "wireless-ssid-contractor")# vlan 40 (ap)(SSID Profile "wireless-ssid-contractor")# auth-server server1 (ap)(SSID Profile "wireless-ssid-contractor")# auth-server server2 (ap)(SSID Profile "wireless-ssid-contractor")# auth-survivability	
7. Create access rule for wired and wireless authentication. In this example, the rule permits all traffic. For contractor SSID role, the rule allows only 10.16.0.0/16 network and all other traffic address is translated at the source and the global routing profile definition is bypassed.	For wired profile: (ap)(config)# wlan access-rule wired-port (ap)(Access Rule "wired-port")# rule any any match any any any permit For WLAN SSID employee roles: (ap)(config)# wlan access-rule wireless-ssid (ap)(Access Rule "wireless-ssid")# rule any any match any any any permit For WLAN SSID contractor roles: (ap)(config)# wlan access-rule wireless-ssid-contractor (ap)(Access Rule "wireless-ssid-contractor")# rule 10.16.0.0 255.255.0.0 match any any any permit (ap)(Access Rule "wireless-ssid-contractor")# rule any any match any any any src-nat	See Configuring Access Rules for Network Services
NOTE: Ensure that you execute the **commit apply** command in the Instant CLI before saving the configuration and propagating changes across the W-IAP cluster.		

AP Connected Switch Configuration

Client VLANs defined in this example must be opened on the upstream switches in multiple AP deployments, as client traffic from slave to master is tagged with the client VLAN.

Datacenter Configuration

For information on controller configuration, see Configuring a Controller for IAP-VPN Operations on page 227. The following OSPF configuration is required on the controller to redistribute IAP-VPN routes to upstream routers.

```
(host)(config) # router ospf
(host)(config) # router ospf router-id <ID>
(host)(config) # router ospf area 0.0.0.0
(host)(config) # router ospf redistribute rapng-vpn
```

Scenario 4 - GRE: Single Datacenter Deployment with No Redundancy

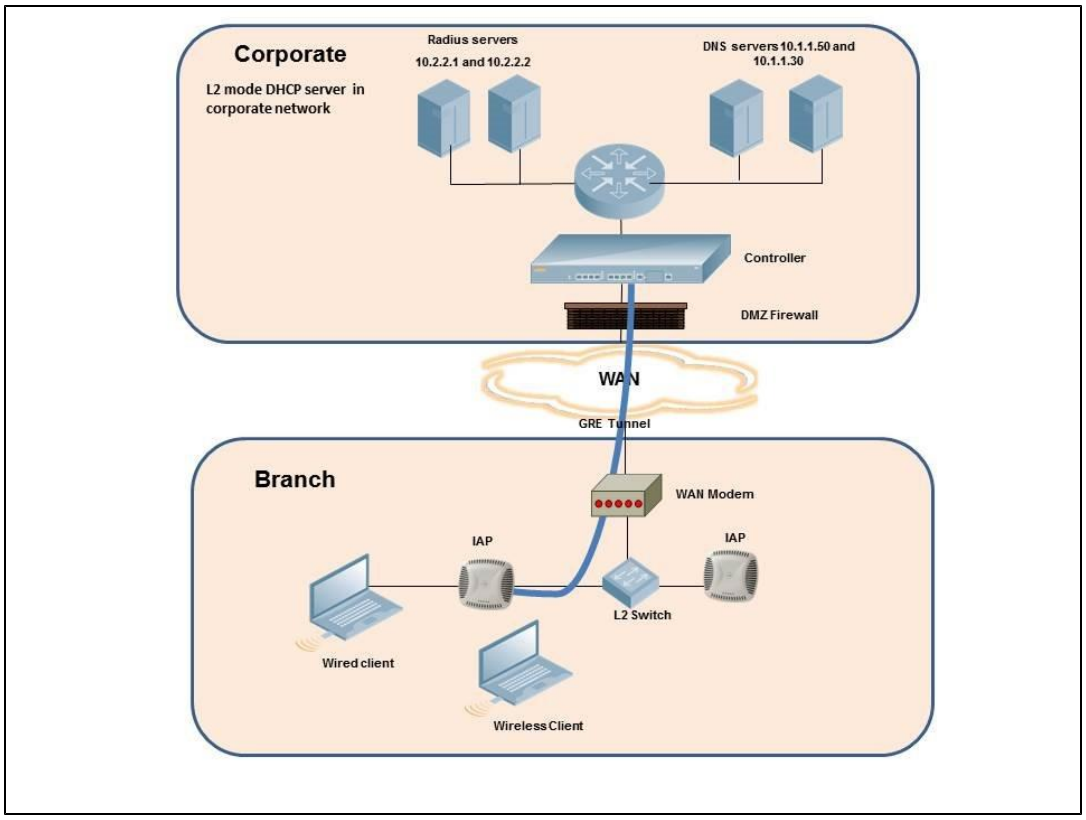
This scenario includes the following configuration elements:

- Single VPN primary configuration using GRE
  - **Aruba GRE**, does not require any configuration on the Dell Networking W-Series Mobility Controller that acts as a GRE endpoint.
  - **Manual GRE**, which requires GRE tunnels to be explicitly configured on the GRE-endpoint that can be a Dell Networking W-Series Mobility Controller or any device that supports GRE termination.
- Tunneling of all traffic to datacenter
- Centralized L2 mode DHCP profile
- RADIUS server within corporate network and authentication survivability for branch survivability.
- Wired and wireless users in L2 mode
- Access rules defined for wired and wireless networks to permit all traffic

Topology

Figure 138 shows the topology and the IP addressing scheme used in this scenario:

Figure 138 *Scenario 4 - GRE: Single Datacenter Deployment with No Redundancy*



The following IP addresses are used in the examples for this scenario:

- 10.0.0.0/8 is the corporate network.
- 10.20.0.0/16 subnet is reserved for L2 mode.

AP Configuration

This section provides information on configuration steps performed through the CLI or the UI.

Table 75: *W-IAP Configuration for Scenario*

Configuration Steps	CLI Commands	UI Procedure

1. Configure Aruba GRE or manual GRE
• Aruba GRE uses an IPSec tunnel to facilitate controller configuration and requires VPN to be configured. This VPN tunnel is not used for any client traffic.
• Manual GRE uses standard GRE tunnel configuration and requires controller configuration to complete the GRE tunnel.
	Aruba GRE configuration
	`(ap)(config)# vpn primary <controller-IP>`
	`(ap)(config)# vpn gre-outside`
	
	Manual GRE configuration
	`(ap)(config)# gre primary <controller-IP>`
	`(ap)(config)# gre type 80`
	
	Per-AP GRE tunnel configuration
	Optionally, per-AP GRE tunnel can also be enabled, which causes each W-IAP to form an independent GRE tunnel to the GRE end-point. This requires each W-IAP MAC to be present in the controller whitelist if Aruba GRE is used, or GRE configuration for the IP of the each W-IAP on the controller for Manual GRE.
	
	`(ap)(config)# gre per-ap-tunnel`
	
	NOTE: Starting with 6.4.0.2-4.1, if Virtual Controller IP is configured and per-AP GRE tunnel is disabled, W-IAP uses Virtual Controller IP as the GRE source IP. For Manual GRE, this simplifies configuration on controller, since only the Virtual Controller IP destined GRE tunnel interface configuration is required.
		See Enabling Automatic Configuration of GRE Tunnel and Manually Configuring a GRE Tunnel

2. Configure routing profiles to tunnel traffic through GRE.	`(ap)(config)# routing-profile` (ap)(routing-profile)# route 0.0.0.0 0.0.0.0 <IP of GRE-endpoint>	See Configuring Routing Profiles
3. Configure Enterprise DNS. The example in the next column tunnels all DNS queries to the client's original DNS server without proxying on W-IAP.	`(ap)(config)# internal-domains` `(ap)(domains)# domain-name *`	See Configuring Enterprise Domains

4. Configure centralized L2 DHCP profile with VLAN 20.	**Centralized L2 DHCP profile VLAN 20**
	`(ap)(config)# ip dhcp l2-dhcp`
	`(ap)(DHCP profile "l2-dhcp")# server-type Centralized,L2`
	`(ap)(DHCP profile "l2-dhcp")# server-vlan 20`
		See Configuring a Centralized DHCP Scope

5. Create authentication servers for user authentication. The example in the next column assumes 802.1x SSID.	`(ap)(config)# wlan auth-server server1`
	`(ap)(Auth Server "server1")# ip 10.2.2.1`
	`(ap)(Auth Server "server1")# port 1812`
	`(ap)(Auth Server "server1")# acctport 1813`
	`(ap)(Auth Server "server1")# key "presharedkey"`
	`(ap)(Auth Server "server1")# exit`
	`(ap)(config)# wlan auth-server server2`
	`(ap)(Auth Server "server1")# ip 10.2.2.2`
	`(ap)(Auth Server "server1")# port 1812`
	`(ap)(Auth Server "server1")# acctport 1813`
	`(ap)(Auth Server "server1")# key "presharedkey"`
		See Configuring an External Server for Authentication

6. Configure wired and wireless SSIDs using the authentication servers	Configure wired ports to operate in centralized L2 mode and associate VLAN 20 to the wired port profile. `(ap)(config) # wired-port-profile wired-port`	See Configuring a Wired Profile

Table 75: *W-IAP Configuration for Scenario*

Configuration Steps	CLI Commands	UI Procedure

and access rules, and enable authentication survivability.	`(ap)(wired-port-profile "wired-port")# switchport-mode access`
	`(ap)(wired-port-profile "wired-port")# allowed-vlan all`
	`(ap)(wired-port-profile "wired-port")# native-vlan 20`
	`(ap)(wired-port-profile "wired-port")# no shutdown`
	`(ap)(wired-port-profile "wired-port")# access-rule-name wired-port`
	`(ap)(wired-port-profile "wired-port")# type employee`
	`(ap)(wired-port-profile "wired-port")# auth-server server1`
	`(ap)(wired-port-profile "wired-port")# auth-server server2`
	`(ap)(wired-port-profile "wired-port")# dot1x`
	`(ap)(wired-port-profile "wired-port")# exit`
	`(ap)(config)# enet1-port-profile wired-port`
	
	Configure a wireless SSID to operate in centralized L2 mode and associate VLAN 20 to the WLAN SSID profile.
	`(ap)(config) # wlan ssid-profile wireless-ssid`
	`(ap)(SSID Profile "wireless-ssid")# enable`
	`(ap)(SSID Profile "wireless-ssid")# type employee`
	`(ap)(SSID Profile "wireless-ssid")# essid wireless-ssid`
	`(ap)(SSID Profile "wireless-ssid")# opmode wpa2-aes`
	`(ap)(SSID Profile "wireless-ssid")# vlan 20`
	`(ap)(SSID Profile "wireless-ssid")# auth-server server1`
	`(ap)(SSID Profile "wireless-ssid")# auth-server server2`
	`(ap)(SSID Profile "wireless-ssid")# auth-survivability`
		and Wireless Network Profiles

7. Create access rule for wired and wireless authentication.	`For wired profile:`
	`(ap)(config)# wlan access-rule wired-port`
	`(ap)(Access Rule "wired-port")# rule any any match any any any`
	`permit`
	
	`For WLAN SSID employee roles:`
	(ap)(config)# wlan access-rule wireless-ssid
	(ap)(Access Rule "wireless-ssid")# rule any any match any any any permit
		See Configuring Access Rules for Network Services

NOTE: Ensure that you execute the **commit apply** command in the Instant CLI before saving the configuration and propagating changes across the W-IAP cluster.		

AP Connected Switch Configuration

Client VLANs defined in this example must be opened on the upstream switches in multiple AP deployments, as client traffic from slave to master is tagged with the client VLAN.

Datacenter Configuration

For information on controller configuration, see Configuring a Controller for IAP-VPN Operations on page 227. The following GRE configuration is required on the controller:

```
(host)(config)# interface tunnel <Number>
```

```
(host)(config-tunnel)# description <Description>
(host)(config-tunnel)# tunnel mode gre <ID>
(host)(config-tunnel)# tunnel source <controller-IP>
(host)(config-tunnel)# tunnel destination <AP-IP>
(host)(config-tunnel)# trusted
(host)(config-tunnel)# tunnel vlan <allowed-VLAN>
```

Acronyms and Abbreviations

The following table lists the abbreviations used in this document.

Table 76: *List of abbreviations*

Abbreviation	Expansion
ARM	Adaptive Radio Management
ARP	Address Resolution Protocol
BSS	Basic Server Set
BSSID	Basic Server Set Identifier
CA	Certification Authority
CLI	Command Line Interface
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
EAP-TLS	Extensible Authentication Protocol- Transport Layer Security
EAP-TTLS	Extensible Authentication Protocol-Tunneled Transport Layer Security
W-IAP	Instant Access Point
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
ISP	Internet Service Provider
LEAP	Lightweight Extensible Authentication Protocol
MX	Mail Exchanger
MAC	Media Access Control
NAS	Network Access Server
NAT	Network Address Translation
NS	Name Server
NTP	Network Time Protocol

Table 76: *List of abbreviations*

Abbreviation	Expansion
PEAP	Protected Extensible Authentication Protocol
PEM	Privacy Enhanced Mail
PoE	Power over Ethernet
RADIUS	Remote Authentication Dial In User Service
VC	Virtual Controller
VSA	Vendor-Specific Attributes
WLAN	Wireless Local Area Network

Glossary

The following table lists the terms and their definitions used in this document.

Table 77: *List of Terms*

Term	Definition
802.11	An evolving family of specifications for wireless LANs developed by a working group of the Institute of Electrical and Electronics Engineers (IEEE). 802.11 standards use the Ethernet protocol and CSMA/CA (carrier sense multiple access with collision avoidance) for path sharing.
802.11a	Provides specifications for wireless systems. Networks using 802.11a operate at radio frequencies in the 5GHz band. The specification uses a modulation scheme known as orthogonal frequency-division multiplexing (OFDM) that is especially well suited to use in office settings. The maximum data transfer rate is 54 Mbps.
802.11b	WLAN standard often called Wi-Fi; backward compatible with 802.11. Instead of the phase-shift keying (PSK) modulation method historically used in 802.11 standards, 802.11b uses complementary code keying (CCK), which allows higher data speeds and is less susceptible to multipath-propagation interference. 802.11b operates in the 2.4 GHz band and the maximum data transfer rate is 11 Mbps.
802.11g	Offers transmission over relatively short distances at up to 54 Mbps, compared with the 11 Mbps theoretical maximum of 802.11b. 802.11g operates in the 2.4 GHz band and employs orthogonal frequency division multiplexing (OFDM), the modulation scheme used in 802.11a, to obtain higher data speed. Computers or terminals set up for 802.11g can fall back to speeds of 11 Mbps, so that 802.11b and 802.11g devices can be compatible within a single network.
802.11n	Wireless networking standard to improve network throughput over the two previous standards 802.11a and 802.11g with a significant increase in the maximum raw data rate from 54 Mbps to 600 Mbps with the use of four spatial streams at a channel width of 40 MHz. 802.11n operates in the 2.4 and 5.0 bands.

Table 77: *List of Terms*

Term	Definition
AP	An access point (AP) connects users to other users within the network and also can serve as the point of interconnection between the WLAN and a fixed wire network. The number of access points a WLAN needs is determined by the number of users and the size of the network.
access point mapping	The act of locating and possibly exploiting connections to WLANs while driving around a city or elsewhere. To do war driving, you need a vehicle, a computer (which can be a laptop), a wireless Ethernet card set to work in promiscuous mode, and some kind of an antenna which can be mounted on top of or positioned inside the car. Because a WLAN may have a range that extends beyond an office building, an outside user may be able to intrude into the network, obtain a free Internet connection, and possibly gain access to company records and other resources.
ad-hoc network	A LAN or other small network, especially one with wireless or temporary plug-in connections, in which some of the network devices are part of the network only for the duration of a communications session or, in the case of mobile or portable devices, while in some close proximity to the rest of the network.
band	A specified range of frequencies of electromagnetic radiation.
DHCP	The Dynamic Host Configuration Protocol (DHCP) is an auto-configuration protocol used on IP networks. Computers or any network peripherals that are connected to IP networks must be configured, before they can communicate with other computers on the network. DHCP allows a computer to be configured automatically, eliminating the need for a network administrator. DHCP also provides a central database to keep track of computers connected to the network. This database helps in preventing any two computers from being configured with the same IP address.
DNS Server	A Domain Name System (DNS) server functions as a phonebook for the Internet and Internet users. It converts human readable computer hostnames into IP addresses and vice-versa. A DNS server stores several records for a domain name such as an address 'A' record, name server (NS), and mail exchanger (MX) records. The Address 'A' record is the most important record that is stored in a DNS server, because it provides the required IP address for a network peripheral or element.
DST	Daylight saving time (DST), also known as summer time, is the practice of advancing clocks, so that evenings have more daylight and mornings have less. Typically clocks are adjusted forward one hour near the start of spring and are adjusted backward in autumn.
EAP	Extensible authentication protocol (EAP) refers to the authentication protocol in wireless networks that expands on methods used by the point-to-point protocol (PPP), a protocol often used when connecting a computer to the Internet. EAP can support multiple authentication mechanisms, such as token cards, smart cards, certificates, one-time passwords, and public key encryption authentication.

Table 77: *List of Terms*

Term	Definition
fixed wireless	Wireless devices or systems in fixed locations such as homes and offices. Fixed wireless devices usually derive their electrical power from the utility mains, unlike mobile wireless or portable wireless which tend to be battery-powered. Although mobile and portable systems can be used in fixed locations, efficiency and bandwidth are compromised compared with fixed systems.
frequency allocation	Use of radio frequency spectrum regulated by governments.
frequency spectrum	Part of the electromagnetic spectrum.
hotspot	A WLAN node that provides Internet connection and virtual private network (VPN) access from a given location. A business traveler, for example, with a laptop equipped for Wi-Fi can look up a local hot spot, contact it, and get connected through its network to reach the Internet and their own company remotely with a secure connection. Increasingly, public places, such as airports, hotels, and coffee shops are providing free wireless access for customers.
IEEE 802.11 standards	The IEEE 802.11 is a set of standards that are categorized based on the radio wave frequency and the data transfer rate.
POE	Power over Ethernet (PoE) is a method of delivering power on the same physical Ethernet wire used for data communication. Power for devices is provided in one of the following two ways: • Endspan– The switch that an AP is connected for power supply. • Midspan– A device can sit between the switch and APs The choice of endspan or midspan depends on the capabilities of the switch to which the W-IAP is connected. Typically if a switch is in place and does not support PoE, midspan power injectors are used.
PPPoE	Point-to-Point Protocol over Ethernet (PPPoE) is a method of connecting to the Internet typically used with DSL services where the client connects to the DSL modem.
QoS	Quality of Service (QoS) refers to the capability of a network to provide better service to a specific network traffic over various technologies.
RF	Radio Frequency (RF) refers to the portion of electromagnetic spectrum in which electromagnetic waves are generated by feeding alternating current to an antenna.
TACACS	Family of protocols that handle remote authentication and related services for network access control through a centralized server.
TACACS+	Derived from TACACS but an entirely new and separate protocol to handle AAA services. TACACS+ uses TCP and is not compatible with TACACS. Because it encrypts password, username, authorization, and accounting, it is less vulnerable than RADIUS.
VPN	A Virtual Private Network (VPN) network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network. A VPN ensures privacy through security procedures and tunneling protocols such as the Layer Two Tunneling Protocol (L2TP). Data is encrypted at the sending end and decrypted at the receiving end.

Table 77: *List of Terms*

Term	Definition
W-CDMA	Officially known as IMT-2000 direct spread; ITU standard derived from Code-Division Multiple Access (CDMA). Wideband code-division multiple access (W-CDMA) is a third-generation (3G) mobile wireless technology that promises much higher data speeds to mobile and portable wireless devices than commonly offered in today's market.
Wi-Fi	A term for certain types of WLANs. Wi-Fi can apply to products that use any 802.11 standard. Wi-Fi has gained acceptance in many businesses, agencies, schools, and homes as an alternative to a wired LAN. Many airports, hotels, and fast-food facilities offer public access to Wi-Fi networks.
WEP	Wired equivalent privacy (WEP) is a security protocol specified in 802.11b, designed to provide a WLAN with a level of security and privacy comparable to what is usually expected of a wired LAN. Data encryption protects the vulnerable wireless link between clients and access points; once this measure has been taken, other typical LAN security mechanisms such as password protection, end-to-end encryption, virtual private networks (VPNs), and authentication can be put in place to ensure privacy.
wireless	Describes telecommunications in which electromagnetic waves (rather than some form of wire) carry the signal over part or all of the communication path.
wireless network	In a Wireless LAN (WLAN), laptops, desktops, PDAs, and other computer peripherals are connected to each other without any network cables. These network elements or clients use radio signals to communicate with each other. Wireless networks are set up based on the IEEE 802.11 standards.
WISP	Wireless ISP (WISP) refers to an internet service provider (ISP) that allows subscribers to connect to a server at designated hot spots (access points) using a wireless connection such as Wi-Fi. This type of ISP offers broadband service and allows subscriber computers, called stations, to access the Internet and the Web from anywhere within the zone of coverage provided by the server antenna, usually a region with a radius of several kilometers.
wireless service provider	A company that offers transmission services to users of wireless devices through radio frequency (RF) signals rather than through end-to-end wire communication.
WLAN	Wireless local area network (WLAN) is a local area network (LAN) that the users access through a wireless connection.